SENATE JUDICIARY COMMITTEE
Senator Thomas Umberg, Chair
2025-2026 Regular Session

AB 1043 (Wicks)
Version: May 23, 2025
Hearing Date: July 15, 2025
Fiscal: Yes
Urgency: No
CK

SUBJECT

Age verification signals: software applications and online services

DIGEST

This bill imposes obligations on covered manufacturers to communicate certain information to developers, including age bracket information, and to obtain parental consent before allowing the download of apps for certain users. The bill requires developers to receive and treat age signals as the primary indicator of the user's age.

EXECUTIVE SUMMARY

Children face numerous serious risks in online environments that can have lasting impacts on their development and wellbeing. Exposure to inappropriate content, including violent, sexual, or disturbing material, can be traumatic and age-inappropriate for developing minds. Cyberbullying and online harassment can lead to anxiety, depression, and social isolation, while predators may attempt to groom or exploit children through social media, gaming platforms, and messaging apps. Additionally, excessive screen time and addictive app design can interfere with sleep, physical activity, and real-world social development. Children may also inadvertently share personal information or fall victim to scams. Many approaches to solving these problems by requiring age verification have serious trade offs, whether it be privacy, security, or effectiveness.

This bill seeks to accomplish these goals by requiring manufacturers of devices, operating systems, and app stores to obtain age information on minor users and to communicate this to app developers. These "covered manufacturers" are required to get parental consent before allowing certain users to download apps from their store, as applicable. Developers are then to treat these signals as the primary indicator of a user's age. This bill is sponsored by Children Now. It is supported by several advocacy groups, including CFT — A Union of Educators & Classified Professionals, and opposed by Chamber of Progress and Lenovo.

PROPOSED CHANGES TO THE LAW

Existing law:

1) Provides a right to free speech and expression. (U.S. Const., 1st amend; Cal. Const., art 1, § 2.)

2) Recognizes certain judicially created exceptions to the rights of freedom of speech and expression. (*E.g., Virginia v. Black* (2003) 538 U.S. 343, 359.)

3) Requires, pursuant to the Parent's Accountability and Child Protection Act, a person or business that conducts business in California, and that seeks to sell any product or service in or into California that is illegal under state law to sell to a minor to, notwithstanding any general term or condition, take reasonable steps, as specified, to ensure that the purchaser is of legal age at the time of purchase or delivery, including, but not limited to, verifying the age of the purchaser. (Civ. Code § 1798.99.1(a)(1).)

4) Establishes the CCPA, which grants consumers certain rights with regard to their personal information, including enhanced notice, access, and disclosure; the right to deletion; the right to restrict the sale of information; and protection from discrimination for exercising these rights. It places attendant obligations on businesses to respect those rights. (Civ. Code § 1798.100 et seq.)

5) Provides a consumer the right, at any time, to direct a business that sells or shares personal information about the consumer to third parties not to sell or share the consumer's personal information. It requires such a business to provide notice to consumers, as specified, that this information may be sold or shared and that consumers have the right to opt out of that selling and sharing. (Civ. Code § 1798.120(a)-(b).)

6) Prohibits a business, notwithstanding the above, from selling or sharing the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers at least 13 years of age and less than 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale or sharing of the consumer's personal information. A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age. (Civ. Code § 1798.120(c).)

7) Establishes the Protecting Our Kids from Social Media Addiction Act, which prohibits an operator of an addictive internet-based service or application from providing an addictive feed to a user unless they have actual knowledge that the

user is not a minor or the operator has obtained parental consent. (Health & Saf. Code § 27000 et seq.)

This bill:

1) Requires a covered manufacturer to provide an accessible interface at account setup that requires an account holder to indicate the birth date, age, or both, of the user of that device for the sole purpose of providing a signal regarding the user's age bracket to applications available in a covered application store.

2) Requires a covered manufacturer that is a covered application store to:
    a) For a user under 16 years of age who has an account holder, obtain account holder consent before permitting the user to download an application made available through the covered application store.
    b) Provide to a developer in the covered application store a signal indicating whether an account holder who is the parent or guardian of a user under 16 years of age has provided such consent.
    c) Provide developers with the ability to disclose to the account holder information or any parental tools provided by the developer.

3) Requires a covered manufacturer to provide developers with a digital signal via a real-time application programming interface (API) identifying the age bracket of the user:
    a) Under five years of age.
    b) At least 5 years of age and under 10 years of age.
    c) At least 10 years of age and under 13 years of age.
    d) At least 13 years of age and under 16 years of age.
    e) At least 16 years of age and under 18 years of age.
    f) At least 18 years of age.

4) Requires a covered manufacturer to send only the minimum amount of information necessary to comply herewith and prohibits the sharing of the digital signal information with a third party for a purpose not required hereby.

5) Provides that a developer that relies in good faith on a signal indicating a user's age provided by a covered manufacturer is presumed to have accurately determined the user's age and to be in compliance with any state law that requires online age verification or parental guardian consent. This presumption is rebuttable by credible evidence that the user's age is different than the signal.

6) Permits a developer that receives a signal indicating a user's age to use that signal to comply with applicable law but shall not do either of the following:
    a) Request more information than the minimum amount of information necessary to comply with this title.

b) Share the signal with a third party for a purpose not required by this title.

7) Subjects a person in violation to an injunction and to liability for a civil penalty of not more than $2,500 per affected child for each negligent violation or not more than $7,500 per affected child for each intentional violation. Such penalties are recoverable only in a civil action brought in the name of the people of the State of California by the Attorney General.

8) Provides that a covered manufacturer that makes a good faith effort to comply herewith, taking into consideration available technology and any reasonable technical limitations or outages, shall not be liable for an erroneous signal indicating a user's age or any conduct by a developer that receives a signal indicating a user's age.

9) Clarifies its scope and interaction with other laws.

10) Includes a severability clause.

11) Defines the relevant terms, including:
    a) "Account holder" means a parent or legal guardian of a user who is under 18 years of age.
    b) "Application" means a software application or online service, product, or feature that may be run or directed by a user on a computer, a mobile device, or any other general purpose computing device. "Online service, product, or feature" does not include a broadband internet access or telecommunications service. This also excludes the delivery or use of a physical product.
    c) "Covered application store" means a publicly available website, software application, online service, or platform that distributes and facilitates the download of applications from third-party developers to users of a computer, a mobile device, or other general purpose computing device.
    d) "Covered manufacturer" means a person who is a manufacturer of a device, an operating system for a device, or a covered application store.
    e) "Developer" means a person that owns, maintains, or controls an application.
    f) "Signal" means age bracket data or notice of parent or guardian consent sent by a real-time secure API or operating system to an application.
    g) "User" means a child that is the primary user of the device.

COMMENTS

1. Age verification concerns

Age verification laws have been pursued across the globe:

> Government agencies, private companies, and academic researchers have spent years seeking a way to solve the thorny question of how to check internet users' ages without the risk of revealing intimate information about their online lives. But after all that time, privacy and civil liberties advocates still aren't convinced the government is ready for the challenge.
>
> "When you have so many proposals floating around, it's hard to ensure that everything is constitutionally sound and actually effective for kids," Cody Venzke, a senior policy counsel at the American Civil Liberties Union (ACLU), tells The Verge. "Because it's so difficult to identify who's a kid online, it's going to prevent adults from accessing content online as well."
>
> In the US and abroad, lawmakers want to limit children's access to two things: social networks and porn sites. Louisiana, Arkansas, and Utah have all passed laws that set rules for underage users on social media. Meanwhile, multiple US federal bills are on the table, and so are laws in other countries, like the UK's Online Safety Bill. Some of these laws demand specific features from age verification tools. Others simply punish sites for letting anyone underage use them — a more subtle request for verification.
>
> Online age verification isn't a new concept. In the US, laws like the Children's Online Privacy Protection Act (COPPA) already apply special rules to people under 13. And almost everyone who has used the internet — including major platforms like YouTube and Facebook — has checked a box to access adult content or entered a birth date to create an account. But there's also almost nothing to stop them from faking it.[1]

A report by France's National Commission on Informatics and Liberty (CNIL) analyzes the various approaches to age verification. It lays out various approaches but cautions that most come with dire flaws:

> With regard to the devices currently available on the market, the CNIL would first like to stress that the effectiveness of age verification tools

[1] Emma Roth, *Online age verification is coming, and privacy is on the chopping block* (May 15, 2023) The Verge, https://www.theverge.com/23721306/online-age-verification-privacy-laws-child-safety.

> depends on the operating rules of the Internet, which is designed as an open network, freely accessible to site users and publishers. While this finding should not prevent the pursuit of the legitimate objectives of protecting minors, care should also be taken to preserve the many benefits linked to this open model (innovation, freedom of expression, user autonomy, etc.). The move towards a closed digital world, where individuals are encouraged to register mainly in authenticated universes (via the creation of user accounts) to avoid a multiplication of identity or identity attribute verifications (age, address, diplomas, etc.) presents significant risks for the rights and freedoms of individuals, which need to be taken into account.
>
> At present, all the solutions proposed can easily be circumvented. Indeed, the use of a simple VPN locating the Internet user in a country that does not require an age verification of this order can allow a minor to bypass an age verification system applied in France, or to bypass the blocking of a website that does not comply with its legal obligations. Similarly, it is difficult to certify that the person using a proof of age is the one who obtained it.
>
> For example, in the UK, where such measures have long been considered, 23% of minors say they can bypass blocking measures and some pornographic content publishers already offer VPN services.
> If the use of VPNs must be subject to a certain vigilance, it should be stressed that such technologies are also one of the essential building blocks of the security of exchanges on the Internet, used by many companies, but also by individuals wishing to protect their browsing from the tracking conducted by public or private stakeholders.[2]

On this latter point, the efficacy of age verification laws on the internet is drastically undercut by the ready access to VPNs. In fact, numerous laws have led to a boom in the industry, as reported by Popular Science in an article entitled "Online porn restrictions are leading to a VPN boom":

> Internet users in a handful of states across the US are finding it more difficult to browse parts of the web anonymously. Over a dozen states, including Texas and Louisiana, have enacted legislation forcing Pornhub and other purveyors of streaming online adult videos to verify the identities of its users to ensure children and teens aren't accessing "sexual material harmful to minors." Elsewhere, in states like Florida, lawmakers have introduced so-called online parental consent laws that would limit or

[2] *Online age verification: balancing privacy and the protection of minors* (September 22, 2022) CNIL, https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors.

> ban underage users from accessing social media services over claims they cause psychological harm. In each case, lawmakers want online platforms to collect government-IDs from users or have them submit to third-party age verification methods to ensure they are indeed adults.
>
> But determining whether or not kids and teens are actually accessing those sites means platforms have no choice but to verify the ages of all users accessing their sites, minor or otherwise. Adult porn viewers, who could previously dip in and out of websites with a relative degree of anonymity, may now fear having their government name and photograph at arms length away from their last Pornhub search query. At the same time, critics of the new laws worry some far-right, religiously conservative lawmakers could broadly interpret "adult" material to include content from LGBTQ+ creators or other people from marginalized groups who rely on the internet for a sense of community. In that scenario, teens from abusive or difficult family structures could find themselves shut out from support structures online.
>
> Experts speaking with PopSci say there are signs internet users in many of these states are turning to Virtual Private Networks (VPNs) to access otherwise blocked materials. Leading VPN provider Top10 VPN claims demand from VPN services jumped 275% on March 15, the same day Pornhub cut off access in Texas. The site says demand for VPNs similarly surged by 210% the day after a similar law took effect in Louisiana last year. ExpressVPN, another popular VPN provider, told PopSci it saw increased web traffic to its site the day anti-porn, online age verification bills took effect in seven out of eight states. . . .
>
> VPNs, which date back to the mid 1990s, create an encrypted tunnel for user's data and can make it appear as if their computer is based in a different geographical location.[3]

2. <u>First Amendment, third rail</u>

The elephant in the room with such age verification laws is the First Amendment to the United States Constitution. The First Amendment, as applied to the states through the Fourteenth Amendment, prohibits Congress or the states from passing any law "abridging the freedom of speech."[4] "[A]s a general matter, the First Amendment means that government has no power to restrict expression because of its message, its ideas, its subject matter, or its content."[5] However, while the amendment is written in

---

[3] Mack Degeurin, *Online porn restrictions are leading to a VPN boom* (April 3, 2024) Popular Science, https://www.popsci.com/technology/vpn-boom/.
[4] U.S. Const., 1st & 14th amends.
[5] *Ashcroft v. American Civil Liberties Union* (2002) 535 U.S. 564, 573.

absolute terms, the courts have created a handful of narrow exceptions to the First Amendment's protections. Expression on the internet is given the same measure of protection granted to in-person speech or statements published in a physical medium.[6]

A constitutional challenge to a restriction on speech is generally analyzed under one of two frameworks, depending on whether the courts deem it to be "content neutral" or "content based," i.e., targeting a particular type of speech. A law is content neutral when it "serves purposes unrelated to the content of the expression."[7] On the other hand, a law is content based when the proscribed speech is "defined solely on the basis of the content of the suppressed speech."[8] If a restriction on speech is determined to be content based, it will be subject to strict scrutiny.[9] A restriction is content based "if it require[s] 'enforcement authorities' to 'examine the content of the message that is conveyed to determine whether' a violation has occurred."[10] Content-based restrictions subject to strict scrutiny are "presumptively unconstitutional."[11] A restriction can survive strict scrutiny only if it uses the least-restrictive means available to achieve a compelling government purpose.[12]

Specifically with reference to regulation of sexual content online, the United States Supreme Court in *Reno v. ACLU* (1997) 521 U.S. 844, 849 invalidated provisions of the Communications Decency Act of 1996 that established criminal penalties for the knowing transmission of obscene or indecent material in a manner likely to be accessible to a minor. Under the statute, an affirmative defense was available to "those who restrict access to covered material by requiring certain designated forms of age proof, such as a verified credit card or an adult identification number or code."[13] Stressing the vagueness and breadth of the statute, the Supreme Court reiterated the principle that the government's interest in protecting children "does not justify an unnecessarily broad suppression of speech addressed to adults."[14] The court also relied on the lower court's findings that there was no effective way to verify a user's age:

> As a practical matter, the Court also found that it would be prohibitively expensive for noncommercial--as well as some commercial--speakers who have Web sites to verify that their users are adults. These limitations must inevitably curtail a significant amount of adult communication on the Internet. By contrast, the District Court found that "despite its limitations, currently available user-based software suggests that a reasonably

[6] *Reno v. ACLU* (1997) 521 U.S. 844, 870.
[7] *Ward v. Rock Against Racism* (1989) 491 U.S. 781, 791.
[8] *FCC v. League of Women Voters* (1984) 468 U.S. 364, 383.
[9] *McCullen v. Coakley* (2014) 573 U.S. 464, 478.
[10] *Id.* at p. 479.
[11] *Reed v. Town of Gilbert* (2015) 135 S.Ct. 2218, 2226 (*Reed*).
[12] *United States v. Playboy Entertainment Group* (2000) 529 U.S. 803, 813.
[13] *Reno,* 521 U.S. at pp. 860-861.
[14] *Id.* at p. 875.

> effective method by which parents can prevent their children from accessing sexually explicit and other material which parents may believe is inappropriate for their children will soon be widely available."[15]

Congress responded by passing the Child Online Protection Act (COPA), which imposed criminal penalties on operators of websites that knowingly post, for commercial purposes, material that is "harmful to minors."[16] An affirmative defense, again, was available for those who take reasonable measures to prevent minors from accessing the website, including age verification.[17] In *Ashcroft v. ACLU* (2004) 542 U.S. 656, the United States Supreme Court affirmed the lower court's ruling that enforcement of the law should be suspended during a pending lawsuit because the statute likely violated the First Amendment. Applying strict scrutiny, the Court found that COPA was likely unconstitutional because content filters installed on computers by parents were less restrictive and more likely to be effective than age verification.[18]

Recently, a Texas law seeking to impose age verification requirements on pornographic websites was challenged, in part, on First Amendment grounds. The United States District Court for the Western District of Texas, relying on *Reno* and *Ashcroft*, subjected the bill to strict scrutiny and found it violated the First Amendment.[19] However, on appeal, the Fifth Circuit Court of Appeals refused to apply the above Supreme Court precedent, and applied a rational basis test, which asks whether a speech restriction is rationally related to the government's legitimate interest, a much less exacting standard.[20] Overturning the lower court's ruling, the court found that the law did not violate the First Amendment. The case was appealed to the U.S. Supreme Court, which, just a few weeks ago, issued its opinion on the case.[21] It applied an entirely different standard, subjecting the law to intermediate scrutiny. The opinion, authored by Justice Clarence Thomas, found that the "power to require age verification is within a State's authority to prevent children from accessing sexually explicit content" and that the Texas law was a constitutionally permissible exercise of that authority. While this law was specifically focused on sexually explicit content, it provides context for the bill at hand.

The First Amendment has been the third rail for a number of laws passed by California in recent years. SB 976 (Skinner, Ch. 321, Stats. 2024) prohibited operators of "internet-based services or applications" from providing "addictive feeds," as those terms are defined, to minors without parental consent and from sending notifications to minors at night and during school hours without parental consent, as provided. SB 976 required

---

[15] *Id.* at pp. 876-877.
[16] *Ashcroft v. ACLU* 542 U.S. at p. 661.
[17] *Id.* at p. 662.
[18] *Id.* at p. 673.
[19] *Free Speech Coal., Inc. v. Colmenero* (W.D. Tex. 2023) 689 F. Supp. 3d 373, 391.
[20] *Free Speech Coal., Inc. v. Paxton* (5th Cir. 2024) 95 F.4th 263.
[21] *Free Speech Coal., Inc. v. Paxton* (2025) 606 U.S. ___ 2025, U.S. LEXIS 2497, *6.

operators to make available to parents a series of protective measures for controlling access to and features of the platform for their children. It also required reporting on data regarding children on their platforms, as specified. Most relevant here, it required operators to reasonably determine that a user is not a minor before providing access. The law was almost immediately challenged and a federal district court has partially enjoined it, finding that elements of the law are likely to infringe upon the First Amendment. However, the court found the challenge to the age assurance provisions not prudentially ripe.[22] The litigation is ongoing.

AB 2273 (Wicks, Ch. 320, Stats. 2022) established the California Age-Appropriate Design Code Act, placing a series of obligations and restrictions on businesses that provide online services, products, or features likely to be accessed by children. This includes a prohibition on using the personal information of any child in a way that the business knows or has reason to know is materially detrimental to the physical health, mental health, or well-being of a child. Relevant here, the law also requires these businesses to "[e]stimate the age of child users with a reasonable level of certainty appropriate to the risks that arise from the data management practices of the business or apply the privacy and data protections afforded to children to all consumers." The law was also challenged on First Amendment grounds. The federal district court applied the facial First Amendment challenge analysis prescribed in *Moody v. NetChoice, LLC* (2024) 603 U.S. 707, a case challenging social media laws in Florida and Texas. The court enjoined much of the law on First Amendment grounds. The plaintiff asserted that the "age estimation requirement would prevent covered businesses from providing expressive content protected by the First Amendment to both children and adults, and likewise would prevent children and adults from accessing expressive content protected by the First Amendment." The court held:

> By requiring a business to estimate age for the purpose of determining what content is appropriate for that age, the CAADCA imposes limits on the content a covered business may publish and the content each user may view. In the alternative, all content must be sanitized to comport with the highest risk level, presumably, the youngest children. Imposing restrictions of that nature with respect to content published to, and accessed by, both children and adults would trigger strict scrutiny of this provision . . . .
>
> The State's argument is grounded in an assumption that greater data privacy for children means greater security and well-being. As NetChoice points out, however, the State ignores that the age estimation requirement will require businesses to collect private information that users may not wish to share. One of NetChoice's declarants, Stacie Rumenap of the nonprofit organization Stop Child Predators, opines that the practical

[22] *NetChoice v. Bonta* (N.D. Cal. 2024) 761 F. Supp. 3d 1202, 1218.

> effect of the CAADCA's age estimation requirement is that businesses will gather and create "a trove of sensitive data" regarding children. Ms. Rumenap considers it "an inevitability, given the realities of data security, that one or more of these data sets will be breached, exposing the personal information of children to bad actors."
> . . .
> On this record, the Court finds that the State has not met its burden to show that age estimation furthers its interest in the privacy and well-being of children.
>
> If a business chooses not to estimate the age of its users, it must apply the privacy and data protections afforded to children to all consumers. However, the Supreme Court has made clear that under the First Amendment, a state "could not reduce the adult population . . . to reading only what is fit for children." "A statute that effectively suppresses a large amount of speech that adults have a constitutional right to receive and to address to one another . . . is unacceptable if less restrictive alternatives would be at least as effective in achieving the legitimate purpose that the statute was enacted to serve." While the State asserts that there are no less restrictive alternatives, it fails to carry its burden on that point because its statement is not supported by any evidence.
>
> Based on the foregoing, the Court finds that § 1798.99.31(a)(5) likely fails strict scrutiny. At the first step of the *Moody* analysis, the Court finds that the provision will impose the same barriers to speech on all covered businesses and their audiences. Every covered business will be forced to choose between intruding into user privacy, thereby chilling publication of and access to protected speech, or publishing only child-appropriate content, thereby restricting access to protected speech for users of all ages. The State has not demonstrate[d] that this choice is narrowly tailored to advance the well-being of children. At the second step of Moody, the Court finds that because all applications of § 1798.99.31(a)(5) will impose barriers to protected speech, the provision has no legitimate sweep.
>
> Accordingly, the Court concludes that NetChoice is likely to prevail on its claim of facial invalidity with respect to California Civil Code § 1798.99.31(a)(5).[23]

3. Establishing the Digital Age Assurance Act

Practical concerns with establishing some level of age assurance have been asserted by the industry. The issue is how each individual developer of applications or online

[23] *NetChoice, LLC v. Bonta* (N.D. Cal. 2025) 769 F. Supp. 3d 1164.

services, products, and features can effectively and appropriately identify the age of users in order to cater their products and services, or to restrict access to them, for children. A recent report by the Family Online Safety Institute (FOSI), an international nonprofit counting many of the major developers and technology companies as members, has teed up the issue:

> As concerns about online safety proliferate, one proposed approach for keeping children safer online is the deployment of age assurance tools capable of estimating or verifying the ages of users. Assessing a person's age online is complicated, particularly when it comes to children and minors. This issue has perplexed the creators of websites, platforms, apps, and games since the early days of the Internet.[24]

FOSI's "Coming to Terms with Age Assurance" report outlines the major challenges in this space:

> **Challenges**
>
> Proportionality
> - Proportionality refers to the use of a risk-based scale to determine which age assurance methods will best minimize online harms to kids.
> - Establishing a risk-based and proportional approach to age assurance is one of the most consistent and important ideas that has coalesced from research, expert interviews, and best practices.
> - The challenge in developing policies around this approach is particularly difficult due to lack of consensus on what the risk levels are for different types of online experiences, and for different ages of kids.
> - It's important to thoughtfully develop a regulatory roadmap that will steadily and reliably reduce harm and uncertainty, rather than mandate a rushed approach.

> Variety of services
> - The tech industry is composed of thousands of companies that offer a variety of services. The challenge of determining a user's age so they can safely access, create, and communicate using those services varies according to the context.
> - There is considerable complexity to the process that must happen internally within companies before the public is ever asked for their

[24] *Coming to Terms with Age Assurance* (July 2023) FOSI, https://fosi.org/wp-content/uploads/2025/03/64b0011a158eea37fb7796c4_FOSI-White-Paper-Coming-to-Terms-with-Age-Assurance-FOR-WEBSITE.pdf.

age. Policy, privacy, and product teams must align in a way that will make age assurance goals possible.

Safety vs. privacy

- A key tension within age assurance is finding a balance between safety and privacy.
- When it comes to age assurance, the more effective a method of verification is, the more data is required. It is not possible to fully verify a person's age without collecting any personal data.
- The variety of methods currently available range from those requiring hard identifiers (such as government issued IDs), to the use of AI and machine learning technologies that can assess an age range. No singular method addresses every concern, and each must be considered individually.

Transparency

- A critical factor in the acceptance of any approach to age assurance will be consumer buy-in.
- Industry will need to convince users that they will only use an individual's identifying information for age estimation purposes and that they will dispose of such information or retain it securely.[25]

This bill seeks to navigate these challenges by placing age assurance responsibility at the manufacturer level. The bill places a series of obligations on "covered manufacturers," defined as manufacturers of devices, operating systems for devices, or covered application stores. "Covered application store" means a publicly available internet website, software application, online service, or platform that distributes and facilitates the download of applications from third-party developers to users of a computer, a mobile device, or any other general purpose computing device. "Application" is broadly defined to mean a software application or online service, product, or feature that may be run or directed by a user on a computer, a mobile device, or any other general purpose computing device.

At account setup, covered manufacturers are required to provide an interface that requires an "account holder," the parent or guardian of a minor user, to indicate the birthdate or age of the user of the relevant device. This information is to be used solely to send a digital signal to a developer, a person that owns, maintains, or controls an application, via a real-time API identifying the relevant age bracket of the minor user. The relevant age brackets are:

- Under 5 years of age.
- 5 to 9 years of age.
- 10 to 12 years of age.
- 13 to 15 years of age.

---

[25] *Ibid.*

- 16 or 17 years of age.
- 18 years of age or older.

If the manufacturer is a covered application store, several additional obligations are imposed. First, if the user is under 16 years of age, the manufacturer must get parental consent before allowing a user to download an application through the covered application store and must communicate whether this consent has been obtained to the developer. These manufacturers must also provide developers with the ability to disclose to the account holder information or any parental tools provided by the developer.

Developers are required to treat these age signals as the primary indicator of a user's age and are deemed to have actual knowledge of the user's age when it receives the signal. A developer with actual knowledge of a user's age is required to connect account holders with any existing tools to support a user with respect to the user's use of the service and as appropriate given the risks that arise from use of the application. The bill establishes a presumption that a developer has accurately determined the user's age and is in compliance with any state law that requires online age verification or parental guardian consent if it relies in good faith on the digital signal provided by a manufacturer. However, this presumption can be rebutted by credible evidence that the user's age is different than that indicated by the manufacturer's signal.

For the privacy and security of users, covered manufacturers must send only the minimum amount of information necessary for compliance herewith. For their part, developers are to use this information to comply with the law but are prohibited from requesting more information than is necessary for compliance. Both manufacturers and developers are prohibited from sharing these digital signals with third parties for any purpose not required by this bill.

A person that violates any of these provisions is subject to an injunction and liable for a modest civil penalty of not more than $2,500 per affected child for each negligent violation or not more than $7,500 per affected child for each intentional violation. Such remedies can only be sought in actions brought by the Attorney General. The bill further provides a broad safe harbor for covered manufacturers who make "a good faith effort to comply," taking into consideration available technology and any reasonable technical limitations or outages. In such instances, the manufacturer is immunized from liability for any erroneous age signal and any conduct by a developer relying on that erroneous signal.

4. A method for age assurance that mitigates age verification concerns

According to the author:

> California's children are growing up with access to an online world that was not built with them in mind. Kids rely on the digital world for education, entertainment, and socialization, but there are no guardrails that protect them from exposure to manipulative design features, and inappropriate interactions. This leaves children vulnerable to harm, including cyberbullying, sextortion, mental health struggles and more. This is simply unacceptable. It is essential that online spaces are designed with children's safety in mind from the outset — and a key part of that design is the ability to accurately assess a user's age.
>
> The Digital Age Assurance Act is a crucial step in ensuring kids can explore the digital world more safely — and a critical step needed for us to require social media and other online companies to implement higher consumer safety standards for products accessed by kids. The urgency behind AB 1043 is backed by mounting evidence of the harmful impacts unregulated digital environments can have on children's mental health, safety, and overall well-being. Creating a statutory age assurance framework that balances privacy and usability will give parents greater peace of mind, build trust with children and families, and create consistency for businesses looking to innovate responsibly. AB 1043 provides a scalable path forward — one that encourages the development of safer online experiences while preserving the benefits of digital participation for young users.

This bill is aimed at avoiding the pitfalls and challenges of the variety of approaches to age verification highlighted above. First, it contains a number of privacy protective features that avoid schemes that might require government identification or invasive biometric data collection. The account holder simply provides the birthdate or age of the user. The manufacturer is the only entity that should receive this specific information. Thereafter, developers are provided the age bracket of the user. Both parties are prohibited from sharing this information for other purposes and no more information than is minimally necessary to comply with the law is allowed to be provided or requested.

Second, it balances the various interests and still maintains a level of reliability, unlike simple self-certification at each point of contact for users. As aptly put in the Assembly Judiciary Committee analysis of the bill:

> Although the age input may not be verified through biometric scans or identity documents, the signal is designed to reflect good-faith entries by a

> parent or guardian and, importantly, cannot later be modified by the user. Minors are therefore unable to change their signal or input false information later in an attempt to bypass parental controls or age-based restrictions. Likewise, developers and applications cannot spoof or overwrite the signal. This infrastructure is intentionally designed to be both privacy-preserving and resistant to circumvention.

Finally, the bill's approach is much more insulated from constitutional challenge than some of its predecessor bills that have sought to protect children online, including AB 2273, discussed above. This bill does not require any restriction be imposed by developers as a result of this information or require any content moderation or design changes. It simply requires developers to connect the relevant account holders with *existing* tools to support a minor user.

The vision of the bill is for these signals to be used to comply with any other laws that require specific treatment of children online. The bill creates certainty by establishing a presumption in favor of developers, providing: "A developer that relies in good faith on a signal indicating a user's age provided by a covered manufacturer is presumed to have accurately determined the user's age and to be in compliance with any state law that requires online age verification or parental guardian consent." However, to ensure the main goals of these laws are properly effectuated, the bill includes a mechanism for rebutting the presumption where there is credible evidence to the contrary. In addition, even if the developer willfully disregards the signal, they will be deemed to have actual knowledge of the user's age.

It should be noted that the provision requiring manufacturers that are application stores to get parental consent before a user under the age of 16 is able to download any application is distinct from the rest of the bill in terms of First Amendment analysis. This provision does specifically limit access to lawful speech and limits the content that can be offered to users based on age. It does not even differentiate between apps that are properly targeted at children or that provide resources for at-risk youth. Therefore, it may be more susceptible to challenge.

Arguably, device-level verification creates a more comprehensive safety net by establishing a framework through which parental controls and content filters can be consistently applied across apps and websites, rather than relying on individual platforms' and developers' varying standards. This approach could enable automatic blocking of inappropriate content, limit data collection from minors, and provide parents with better visibility and control over their children's digital experiences. Furthermore, device-level age verification could facilitate access to educational content and age-appropriate social features while maintaining stronger privacy protections, ultimately creating a more secure digital environment that supports healthy child development without completely restricting beneficial online activities.

5. Stakeholder concerns

Concerns have been raised about various components of this proposed regulatory framework. Some stakeholders have called for provisions that more specifically spell out the technical details regarding the digital interactions between covered manufacturers and developers. In response, the author has agreed to amendments that make clear a covered manufacturer is to provide developers a user's age bracket signal *when the developer requests the signal*. The developer is required to so request the signal when a user requests to download an application. The developer is then deemed to have actual knowledge of the user's age across all platforms of the application and points of access of the application.

Other stakeholders have asked for amendments that ensure developers can continue to enforce their terms of service relating to age restrictions. Several stakeholders have requested express carve outs where certain age assurance protocols are already in place or, in the alternative, amendments that significantly scale back the definitions of developer, application, and/or covered application store.

One concern in particular is with the scope of the definition of "application" to include an "online service, product, or feature." In response, the author has agreed to amendments that remove this portion of the definition, narrowing significantly the scope of the bill. The understanding is this is being done to allow more time to properly address technical concerns with applying the provisions of this bill so broadly.

Writing in opposition, Chamber of Progress argues:

> While it is important to encourage parental involvement to ensure minors' safety online, parents are not always best suited to control how their child uses a platform. AB 1043 risks harming the very children it aims to protect, especially vulnerable youth. Many apps that provide critical services, such as platforms supporting mental, physical, and reproductive health, prioritize anonymity to ensure user safety and promote positive, help-seeking behaviors. Age-bracket signaling and automatic parental consent and control requirements, as outlined in AB 1043, could pressure app stores to collect more information, compromising privacy.
>
> In situations where a parent does not support their child's identity or seeks to restrict access to certain political, health, or other information, this authority can be utilized and weaponized as a tool of control, particularly in abusive or unhealthy home environments. For many youth, online spaces serve as a lifeline, offering access to communities, resources, and support networks that may not be available in their offline lives. LGBTQ+ youth, especially those who may live in communities hostile to their identity, see social media as a crucial tool to connect with LGBTQ+

> groups, access content from people's shared experiences, maintain positive connections, and reduce perceived isolation. LGBTQ+ youth use online platforms to seek emotional support, search for information about their identities, and find communities that accept them when their own parents do not. In fact, only 38% of LBGTQ youth report living in affirming households, while 60% reported finding online spaces to be supportive.

In response to these concerns, and the First Amendment implications discussed above, the author has agreed to amendments that remove the parental consent requirements in the bill, and the attendant provisions regarding connecting account holders with existing tools.

6. Stakeholder support

Children Now, the sponsor of the bill, writes:

> The mental health of youth is in crisis. The challenges that families have faced for generations are exacerbated and amplified by modern technology. Parents, schools and governments are all grappling with the challenges of how to keep kids safe online. Simultaneously, connectivity provides opportunity for access to friends, family, community, and resources.
>
> By sharing approximate users' age to developers of online products and services, AB 1043 will ensure that online platforms provide age-appropriate online experiences. AB 1043 marks an important step toward creating a developmentally safe online world that supports youths' mental, emotional, and social development.

CFT writes in support:

> Young people are struggling like never before. Challenges families have faced for generations are now intensified by modern technology, exposing young people to cyberbullying, sextortion, trafficking, harmful drugs, and abuse, both online and offline. Behind the screen, platforms mine the personal data of young people to build complex profiles used for targeted advertising and to addict kids to their screens. At the same time, connectivity offers valuable opportunities for connection, community and support. AB 1043 offers a responsible, secure, privacy-first solution that protects young people while preserving those benefits.

SUPPORT

Children Now (sponsor)
California Catholic Conference
California Civil Liberties Advocacy
California Parents for Public Virtual Education
CFT- a Union of Educators & Classified Professionals, AFT, AFL-CIO
#HalfTheStory
Parent Support for Online Learning
The Source LGBT+ Center

OPPOSITION

Chamber of Progress
Lenovo, Inc.

RELATED LEGISLATION

Pending Legislation:

AB 2 (Lowenthal, 2025) increases the penalties that can be sought against a social media platform, as defined, if the platform fails to exercise ordinary care or skill and injures a child. AB 2 is currently in this Committee and is set to be heard the same day as this bill.

AB 56 (Bauer-Kahan, 2025) requires social media platforms to clearly display warning labels about the harms associated with social media when users enter the platform and after extended use, as provided. AB 56 is currently in the Senate Health Committee.

Prior Legislation:

SB 976 (Skinner, Ch. 321, Stats. 2024) *See* Comment 2.

AB 1949 (Wicks, 2024) would have prohibited collecting, sharing, selling, using, or disclosing the personal information of minors without affirmative consent from either the minor or their parent or guardian, as provided. It would have required businesses to treat a consumer as under 18 years of age if the consumer, through a platform, technology, or mechanism, transmits a signal indicating that the consumer is less than 18 years of age. AB 1949 was vetoed by Governor Newsom, who stated: "[T]his bill would fundamentally alter the structure of the CCPA to require businesses, at the point of collection, to distinguish between consumers who are adults and minors. I am concerned that making such a significant change to the CCPA would have unanticipated and potentially adverse effects on how businesses and consumers interact with each other, with unclear effects on children's privacy."

AB 3080 (Alanis, 2024) would have required a person or business that makes available products that are illegal to make available to minors, including pornographic internet websites, to take reasonable steps to ensure the user is of legal age at the time of access, including by verifying the age of the user. AB 3080 died in the Senate Appropriations Committee.

AB 2273 (Wicks, Ch. 320, Stats. 2022) *See* Comment 2.

PRIOR VOTES:

Assembly Floor (Ayes 76, Noes 0)
Assembly Appropriations Committee (Ayes 11, Noes 0)
Assembly Judiciary Committee (Ayes 12, Noes 0)
Assembly Privacy and Consumer Protection Committee (Ayes 13, Noes 0)
****