SENATE PRIVACY, DIGITAL TECHNOLOGIES, AND CONSUMER PROTECTION COMMITTEE
Senator Christopher Cabaldon, Chair
2025-2026 Regular Session

AB 1856 (Wicks)
Version: May 18, 2026
Hearing Date: June 22, 2026
Fiscal: Yes
Urgency: No
BD/CK

SUBJECT

Age verification signals: software applications and online services

DIGEST

This bill updates the Digital Age Assurance Act by clarifying the scope of the Act and expanding the Act to apply to browsers and websites.

EXECUTIVE SUMMARY

As the internet has facilitated the widespread distribution of inappropriate, exploitative, and harmful content to minors, lawmakers have long grappled with the issue of online age verification. Solutions ranged from simply asking users to confirm they were adults to requiring users to upload government-issued identification, each containing its own trade-offs. Last year, the Legislature passed AB 1043 (Wicks, Ch. 675, Stats. 2025), which established the Digital Age Assurance Act. The act created a framework for device-based verification for users of mobile devices and computers. AB 1043 required that operating system providers communicate age bracket information to developers. The bill further required developers to request and treat age signals as the primary indicator of the user's age. Once AB 1043 was signed into law, the Governor released a signing message, urging the Legislature to address operational concerns of streaming services and video game developers.

This bill responds to that signing message and expands the Act. It clarifies that requirements of the Act apply to child users who are the primary users of a device. The bill further expands the Act to apply to browsers and websites, as specified, thereby significantly expanding the framework. The bill also makes several clean-up changes.

This bill is author-sponsored and supported by groups such as Children Now and Common Sense Media. It is opposed by groups, including the Electronic Frontier Foundation and the Chamber of Progress.

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.)

8) Establishes the Digital Age Assurance Act. (Civ. Code § 1798.500 et seq.)

9) Defines key terms, including:
    a) "Account holder" means an individual who is at least 18 years of age and a parent or legal guardian of a user who is under 18 years of age in this state.
    b) "Age bracket data" means nonpersonally identifiable data derived from a user's birth date or age for the purpose of sharing with developers of applications that indicates the user's age range, including, at a minimum, whether the user is under 13, between 13 and 16, between 16 and 18, or at least 18.
    c) "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 that can access a covered application store or can download an application.
    d) "Developer" means a person who owns, maintains, or controls an application.
    e) "Operating system provider" means a person or entity that develops, licenses, or controls the operating system software on a computer, mobile device, or any other general purpose computing device.
    f) "Signal" means age bracket data sent by a real-time secure application programming interface or operating system to an application.
    g) "User" means a child under the age of 18 who is the primary user of the device. (Civ. Code § 1798.500.)

10) Requires an operating system provider to do all of the following:
    a) 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 purpose of providing a signal regarding the user's age bracket to applications available in a covered application store.
    b) Provide a developer who has requested a signal with respect to a particular user with a digital signal via a reasonably consistent real-time application programming interface that identifies whether the user is under 13, between 13 and 16, between 16 and 18, or at least 18.
    c) Send only the minimum amount of information necessary to comply with the Act and not share the digital signal information with a third party for a purpose not required by the Act. (Civ. Code § 1798.501(a).)

11) Requires developers to request a signal with respect to a particular user from an operating system provider or a covered application store when the application is downloaded and launched.
    a) Deems a developer who receives a signal to actual knowledge of the user's age range.
    b) Prohibits a developer from willfully disregarding internal clear and convincing information otherwise available to the developer that indicates the user's age is different than the signal indicates.
    c) Requires a developer to treat a signal as the primary indicator of a user's age range unless the developer has internal clear and convincing information that the user's age differs from that indicated by the signal, in which case the developer must use that information as the primary indicator of the user's age.
    d) Prohibits a developer that receives an age signal from requesting more information from an operating system provider or a covered application store than the minimum amount of information necessary to comply with the Act, and from sharing the signal with a third party not required by the Act. (Civ. Code § 1798.501(b).)

12) Requires an operating system provider, with respect to a device for which account setup was completed before January 1, 2025, to provide an accessible interface that allows an account holder to indicate the birth date, age, or both, of the user of that device for the purpose of providing a signal regarding the user's age bracket to applications available in a covered application store. (Civ. Code § 1798.502(a).)

13) Requires a developer, if the application is updated on or after January 1, 2026, or downloaded before January 1, 2027, to request a signal from a covered application store with respect to a user of the device before July 1, 2027. (Civ. Code § 1798.502(b).)

14) Subjects violators to civil penalties for each affected child of up to $2,500 for negligent violations and $7,500 for intentional violations, in an action brought by the Attorney General. Excuses operating system providers and covered application stores from liability for erroneous signals and conduct by developers that receive signals, if the operating system provider or covered application store makes a good faith effort to comply with the Act. (Civ. Code § 1798.503.)

This bill:

1) Modifies and adds the following definitions to the Digital Age Assurance Act:
    a) Specifies that "application" does not include software components that are not themselves offered to consumers as a stand-alone executable application through a covered application store.

b) "Browser" means an application that enables a user to visit an internet website.
c) "Browser provider" means a person or entity that controls or operates a browser for use on a computer, mobile device, or any other general-purpose computing device.
d) "Developer" means a person who owns an application or maintains or controls the hosting of the application in a covered application store.
e) "Internet website operator" means a person that owns, maintains, or controls an internet website that is subject to a law that requires the internet website operator to verify the age of users.
f) Specifies that "operating system provider" does not mean a person or entity that distributes an operating system or application under license terms that permit a recipient to copy, redistribute, and modify the software.
g) "Signal" means age bracket data that pertains to the primary user of a device that is either sent by a real-time secure application programming interface or operating system to an application or communicated by a browser provider to an internet website operator in any technically feasible manner.

2) Deletes the definition of "user" and specifies that the obligations of the Digital Age Assurance Act only apply to the primary user of a device.

3) Expands the Digital Age Assurance Act to apply to browser providers and website operators, including by:
   a) Requiring an operating system provider to provide an accessible interface to indicate a primary user's age to a browser provider and internet website operator.
   b) Requiring an operating system provider to provide a signal that indicates a user's age bracket to a covered application store and browser provider that has requested a signal.
   c) Requiring internet website operators to request a signal from the user's browser provider when the user accesses the internet.
   d) Expanding the provision that deems a developer to have actual knowledge of the age range of the user to whom that signal pertains, even if the developer willfully disregards the signal, to internet website operators.
   e) Expanding data minimization requirements to internet website operators.

4) Specifies that an operating system provider is required to provide an accessible interface to indicate an age signal and an age bracket signal to entities only if the operating system provider's operating system has an account setup feature.

5) Requires a covered application store to do both of the following with respect to a user of the covered application store:
   a) Request a signal from the user's operating system provider.
   b) Provide the signal to a developer upon request.

6) Requires a browser provider to do both of the following with respect to a user of the browser:
    a) Request a signal from the user's operating system provider.
    b) Provide the signal to an internet website upon request.

7) Clarifies that a developer shall request a signal from an operating system provider or covered application store when the application is downloaded onto, and launched from, a particular device.

8) Prohibits entities from prompting the user to change their age information.

9) Removes the provision that deems an entity receiving the signal as having actual knowledge of a user's age across all platforms and points of access of an application.

10) Clarifies that developers or internet website operators that have internal clear and convincing information that a user's age is different than the age indicated by the signal, the developer or internet website provided shall be deemed to have actual knowledge of the user's age range.

11) Provides, for the purposes of the above provision, "clear and convincing information" includes, but is not limited to, age information shared with a developer or internet website operator by an account holder regarding the age of a user of a subaccount of the primary account of the account holder or age information shared with the developer by an account holder regarding the age of the user associated with the account.

COMMENTS

1. Age verification, broadly

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 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

[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.

> 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 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

[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.

> 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. Legislative history: AB 1043

In 2025, the Legislature passed AB 1043 (Wicks, Ch. 675, Stats. 2025), which created an age verification framework to thread the needle between the various benefits and downsides of alternative forms of age verification. AB 1043 required an operating system provider to provide an accessible interface at account setup that requires an account holder to indicate age information of the user of that device for the purpose of providing a signal regarding the user's age bracket to applications available in a covered application store. Such providers must also respond to developers of applications that have requested a signal with respect to a particular user with a digital signal via a reasonably consistent real-time application programming interface (API) that identifies, at a minimum, the user's age bracket, as provided.

For their part, developers are required to request such a signal from the operating system provider or a covered application store when the relevant application is downloaded and launched. The signal so provided must be treated as the primary indicator of a user's age range for purposes of determining the user's age. Importantly, a developer that receives such a signal is deemed to have actual knowledge of the age range of the user to whom that signal pertains across all platforms of the application and points of access of the application, even if the developer willfully disregards it.

Importantly, AB 1043's provisions were limited to operating system providers. It did not apply to the internet writ large or websites. In signing AB 1043 into law, the Governor gave the following message:

---

[3] Mack Degeurin, *Online porn restrictions are leading to a VPN boom* (April 3, 2024) Popular Science, https://www.popsci.com/technology/vpn-boom/.

> I am signing Assembly Bill 1043, which would establish a much-needed system of age verification for users of mobile devices and computers. Parents who allow their children to be the main user of a device will be able to configure the device to inform application developers of the child's age. This, in turn, will assist parents in ensuring that their children are downloading and using age-appropriate applications.
>
> Streaming services and video game developers contend that this bill's framework, while well-suited to traditional software applications, does not fit their respective products. Many of these companies have existing age verification systems in place, addressing complexities such as multi-user accounts shared by a family and user profiles utilized across multiple devices. As this bill does not take effect until January 1, 2027, I urge the Legislature to enact legislation in 2026 to address these particular concerns.

3. Responding to the Governor and expanding the scope of the Act

This bill both responds to this signing message and expands the scope of AB 1043. Specifically, rather than carving out streaming services and video game developers, the bill refocuses the Act's provisions to apply to the primary user of a device.

Operating system providers[4] whose system has an account setup features on a particular device must now provide the accessible interface to not only a covered application store and developers of applications in a covered application store, but also browser providers and website operators. It should be noted that the latter category applies only to websites that are subject to a law that requires the website operator to verify the age of users.

Operating system providers must provide age signals to developers, app stores, and browser providers that request them. Covered app stores and browser providers must request the age signals and provide them, upon request, to developers and website operators, respectively. In turn, the website operators are required to request the signal when a user accesses their website. To prevent circumvention, these entities are prohibited from prompting the user to change the user's age information.

Interestingly, the bill removes the provision that deems an entity receiving the signal as having actual knowledge of a user's age across all platforms and points of access of an application.

[4] The bill also carves out of the definition of "operating system provider" a person or entity that distributes an operating system or application under license terms that permit a recipient to copy, redistribute, and modify the software.

The bill responds to some of the concerns raised with respect to AB 1043 by providing that a developer or website operator hat has internal clear and convincing information that a user's age is different than the age indicated by the signal received, the entity shall use that information as the primary indicator of the user's age and shall be deemed to have actual knowledge of the age range of the user to what the information pertains. The bill now defines "clear and convincing information" as including age information shared with a developer or website operator by an account holder regarding the age of a user of a subaccount of the primary account of the account holder or age information shared with a developer by an account holder regarding the age of a user associated with the account.

According to the author:

> Last year's bill, AB 1043, creates a consistent, privacy-first pathway to online age assurance — giving families the confidence that tech platforms can build the right protections for kids into their products without interfering with an app's existing account features, user settings, or ability to set parental controls. This age assurance framework establishes actual knowledge of users' age range in order for these applications to abide by applicable laws, including California's groundbreaking privacy laws. In order to provide additional guidance for age assurance, AB 1856 would clarify provisions for implementing the age assurance framework and also integrate websites into this framework.

4. Opposition concerns

Opposition raises a number of concerns with the bill, asserting the expansion of the scope of the Digital Age Assurance Act is unwieldy and legally risky. Writing in opposition, Chamber of Progress asserts:

> AB 1043 worked in part because app stores are centralized environments where operating systems can reliably mediate interactions between users and apps. Extending that same model to websites and online services is fundamentally different, more like applying app store-style rules to the broader web, where access is more fragmented and not always tied to a single operating system. In practice, this could lead to less consistent implementation across devices and browsers, create pressure for broader forms of age verification, and expand the system beyond its original child safety focus. Rather than targeting a specific, high-leverage point in the ecosystem, this change risks turning a focused framework into a more pervasive internet-wide layer without clear evidence of improved outcomes. Furthermore, because the proposed amendments sweep in "online service[s], product[s], [and] feature[s]" without clearly defining

> these terms, the changes may render the law void for vagueness in violation of the Fifth and Fourteenth Amendments to the United States Constitution.

The Electronic Frontier Foundation (EFF) also raises scoping concerns:

> A.B. 1856 would extend A.B. 1043's age-signaling framework beyond the app and app store ecosystem and into the broader web, requiring browsers and websites to participate in the collection and transmission of age-related information. Doing so would significantly increase the number of entities involved in processing users' sensitive personal information, thereby amplifying the privacy and security risks. It would also bring a far broader range of online speech within the scope of California's age-bracketing regime, burdening the rights of adults and minors alike.
>
> To address these concerns, we therefore urge the Legislature to amend A.B. 1856 to eliminate the expansion of the age-signaling framework beyond operating systems, application stores, and application developers. Specifically, browser providers and internet website operators should be removed from the list of entities authorized or required to receive age signals from operating systems under this bill.

EFF also highlights in its opposition letter privacy and equity implications of the bill:

> The legislature passed A.B. 1043 in the last legislative session, which creates a blanket mechanism that would impose age gates on all app store users, for every application they download. This creates unnecessary barriers for all users who may not want or need to verify their age simply to access apps—like dictionary apps, map apps, or school resource platforms—with no harmful content or functions.
>
> Under A.B. 1043, manufacturers will be required to track and manage users' ages, leading to the collection and storage of even more sensitive personal data. Although A.B. 1043 limits the use and disclosure of this personal information, it is an unfortunate reality that it could easily be misused or inadvertently exposed. It also forces all apps into rigid age brackets that do not reflect the diversity and flexibility of all users' needs. This bracketed approach disregards the many nuanced and context-dependent ways in which digital tools are used, and disproportionately impacts vulnerable communities, such as low-income households where a single device may be used by multiple people of different ages.

> In its current form, A.B. 1856 does not fix these flaws. Instead, it extends the age-gating regime to browsers and websites, dramatically broadening its scope and pulling more services, developers, and users into an anonymity- and privacy-destroying data collection framework that has not yet been implemented or evaluated.

5. Support

Supporters laud the bill for filling in the gaps left by AB 1043. Common Sense Media writes:

> Children do not experience the internet in silos. They move fluidly between apps, browsers, websites, and cross-platform services. AB 1856 closes critical gaps by ensuring that age-assurance signals follow the child across all of these environments, so platforms cannot avoid applying youth protections simply because a child accesses content through a different pathway.
>
> AB 1856 makes several essential improvements to the Digital Age Assurance Act:
>
> - Creates a consistent, interoperable age-assurance system by requiring operating systems with account-setup features to transmit age-bracket signals to app stores, developers, browsers, and website operators.
> - Expands the Act to browser providers and website operators, ensuring that all online environments where children access content are covered.
> - Requires data minimization, directing operating systems to send only the minimum information necessary to comply with the law.
> - Clarifies actual knowledge, specifying that developers and website operators have actual knowledge of a user's age when they receive an age-bracket signal, while allowing "clear and convincing information" to override the signal when appropriate.
> - Addresses multi-user and family-account scenarios, resolving implementation issues raised by streaming services and other platforms that rely on subaccounts or shared devices.
>
> These updates reflect how children actually navigate online spaces and ensure that California's age-assurance framework remains privacy-protective, technically workable, and aligned with the state's broader child-safety and privacy laws.

Writing in support, Children Now highlights the need for the bill:

> Protecting children from exploitation and abuse, both online and offline, is central to our whole-child mission. California has led the nation in requiring social media platforms to maintain accessible mechanisms for reporting CAM and other harmful content. Despite this, research has documented that major platforms continue to avoid these legal obligations through confusing, multi-step reporting systems that are intentionally difficult to navigate, particularly for young people on mobile devices. A 2025 report by the Children's Advocacy Institute at the University of San Diego School of Law, Child Cruelty by Design, evaluated four platforms (Instagram, Facebook, Snapchat, and TikTok) and found that all four undermined California's existing laws establishing standards for users to report CAM and seek relief from cyberbullying.
>
> Even companies that are among the world's foremost experts in user interface design have built reporting mechanisms that are confusing, multi-step, and inaccessible, making it harder for users to flag CSAM, sexual exploitation, cyberbullying, and other violations. This is not an accident: it is a design choice, and it puts children at risk.

SUPPORT

California Catholic Conference
Children Now
Common Sense Media
Elevate California
Los Angeles Unified School District

OPPOSITION

Chamber of Progress
Electronic Frontier Foundation
Motion Picture Association of America
4 Individuals

RELATED LEGISLATION

AB 1709 (Lowenthal, 2026) prohibits "covered platforms" that provide addictive feeds from allowing users under the age of 16 to create or maintain an account. The Attorney General (AG) may adopt regulations, as provided. It establishes the e-Safety Advisory Commission to advise the AG on, among other things, implementation and enforcement. AB 1709 is set to be heard in this Committee the same day as this bill.

AB 1043 (Wicks, Ch. 675, Stats. 2025) *See* Comment 2.

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 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. This law is the subject of ongoing litigation.

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.

PRIOR VOTES:

Assembly Floor (Ayes 68, Noes 1)
Assembly Appropriations Committee (Ayes 11, Noes 0)
Assembly Privacy and Consumer Protection Committee (Ayes 13, Noes 1)

****