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

AB 2246 (Wicks)
Version: April 23, 2026
Hearing Date: June 15, 2026
Fiscal: Yes
Urgency: No
CK

SUBJECT

Online service, product, or feature: access by children

DIGEST

This bill replicates portions of the California Age-Appropriate Design Code Act (AADC), removing provisions found unconstitutional by federal courts.

EXECUTIVE SUMMARY

AB 2273 (Wicks, Ch. 320, Stats. 2022) established the AADC, 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. 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 AADC requires specified businesses to perform data protection impact assessments (DPIA) and to provide default privacy settings and other protections. The law also calls for the creation of a Children's Data Protection Working Group (CDPWG) tasked with delivering a report on best practices for AADC implementation. Violations are enforceable by the Attorney General. The law was challenged shortly after going into effect and although a number of opinions have been issued from the Ninth Circuit, the legal battle continues. Those opinions have upheld certain provisions of the law but found others unconstitutional.

This bill replicates the AADC but excises the parts found unconstitutional and further narrows other provisions. It is sponsored by Children Now. It is supported by the American Academy of Pediatrics, California, among other groups. It is opposed by several industry associations. Should it pass out of this Committee, it will next be heard by the Senate Judiciary Committee.

PROPOSED CHANGES TO THE LAW

Existing law:

1) Establishes the federal Children's Online Privacy Protection Act (COPPA) to provide protections and regulations regarding the collection of personal information from children under the age of 13. (15 U.S.C. § 6501 et seq.)

2) Establishes the AADC. (Civ. Code § 1798.99.28 et seq.)[1]

3) Defines relevant terms within the AADC, including:
    a) "Child or children" means a consumer or consumers under 18 years of age.
    b) "Data Protection Impact Assessment" (DPIA) means a systematic survey to assess and mitigate risks that arise from the data management practices of the business to children who are reasonably likely to access the online service, product, or feature at issue that arises from the provision of that online service, product, or feature.
    c) "Default" means a preselected option adopted by the business for the online service, product, or feature.
    d) "Likely to be accessed by children" means it is reasonable to expect, based on the following indicators, that the online service, product, or feature would be accessed by children:
    e) The online service, product, or feature is directed to children as defined by the Children's Online Privacy Protection Act (15 U.S.C. Sec. 6501 et seq.).
    f) The online service, product, or feature is determined, based on competent and reliable evidence regarding audience composition, to be routinely accessed by a significant number of children.
    g) An online service, product, or feature with advertisements marketed to children.
    h) An online service, product, or feature that is substantially similar or the same as an online service, product, or feature subject to (ii).
    i) An online service, product, or feature that has design elements that are known to be of interest to children, including, but not limited to, games, cartoons, music, and celebrities who appeal to children.
    j) A significant amount of the audience of the online service, product, or feature is determined, based on internal company research, to be children.
    k) "Profiling" means any form of automated processing of personal information that uses personal information to evaluate certain aspects relating to a natural person, including analyzing or predicting aspects concerning a natural person's performance at work, economic situation,

[1] All further statutory references are to the Civil Code unless specified otherwise.

health, personal preferences, interests, reliability, behavior, location, or movements. (§ 1798.99.30.)

4) Requires a business that provides an online service, product, or feature likely to be accessed by children to take all the following actions:
    l) Before offering a new online service, product, or feature to the public, complete a DPIA. The business must biennially review the DPIA and maintain documentation of the assessment as long as the online service, products, or features are likely to be accessed by children. A DPIA must address the following, as applicable:
        i. Whether the design of the online product, service, or feature could harm children, including by exposing children to harmful, or potentially harmful, content on the online product, service, or feature.
        ii. Whether the design of the online product, service, or feature could lead to children experiencing or being targeted by harmful, or potentially harmful, contacts on the online product, service, or feature.
        iii. Whether the design of the online product, service, or feature could permit children to witness, participate in, or be subject to harmful, or potentially harmful, conduct on the online product, service, or feature.
        iv. Whether the design of the online product, service, or feature could allow children to be party to or exploited by a harmful, or potentially harmful, contact on the online product, service, or feature.
        v. Whether algorithms used by the online product, service, or feature could harm children.
        vi. Whether targeted advertising systems used by the online product, service, or feature could harm children.
        vii. Whether and how the online product, service, or feature uses system design features to increase, sustain, or extend use of the online product, service, or feature by children, including the automatic playing of media, rewards for time spent, and notifications.
        viii. Whether, how, and for what purpose the online product, service, or feature collects or processes sensitive personal information of children.
    m) Make DPIAs available to the Attorney General within 5 days of a request, as specified.
    n) Document any risk of material detriment to children that arises from the data management practices of the business identified in the DPIA and create a timed plan to mitigate or eliminate the risk before the online service, product, or feature is accessed by children.

o) Estimate 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.
p) Configure all default privacy settings provided to children by the online service, product, or feature to settings that offer a high level of privacy, unless the business can demonstrate a compelling reason that a different setting is in the best interests of children.
q) Provide any privacy information, terms of service, policies, and community standards concisely, prominently, and using clear language suited to the age of children likely to access that online service, product, or feature.
r) If the online service, product, or feature allows the child's parent, guardian, or any other consumer to monitor the child's online activity or track the child's location, provide an obvious signal to the child when the child is being monitored or tracked.
s) Enforce published terms, policies, and community standards established by the business, including, but not limited to, privacy policies and those concerning children.
t) Provide prominent, accessible, and responsive tools to help children, or if applicable their parents or guardians, exercise their privacy rights and report concerns. (§ 1798.99.30(a).)

5) Prohibits a business that provides an online service, product, or feature likely to be accessed by children from taking any of the following actions:
u) 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.
v) Profiling a child by default unless (1) the business can demonstrate it has appropriate safeguards in place to protect children, and (2) profiling is necessary for the service, product or feature, and the business can demonstrate a compelling reason that profiling is in the best interests of children.
w) Collect, sell, share, or retain any personal information that is not necessary to provide an online service, product, or feature with which a child is actively and knowingly engaged, unless the business can demonstrate a compelling reason that doing so is in the best interests of children.
x) Use personal information for any reason other than a reason for which that personal information was collected, unless the business can demonstrate a compelling reason that use of the personal information is in the best interests of children.
y) Collect, sell, or share any precise geolocation information of children by default unless the collection of that precise geolocation information is strictly necessary for the business to provide the service, product, or

feature requested and then only for the limited time that the collection of precise geolocation information is necessary to provide the service, product, or feature.

z) Collect any precise geolocation information of a child without providing an obvious sign to the child for the duration of that collection that precise geolocation information is being collected.

aa) Use dark patterns to lead or encourage children to provide personal information beyond what is reasonably expected to provide that online service, product, or feature, to forego privacy protections, or to take any action that the business knows, or has reason to know, is materially detrimental to the child's physical health, mental health, or well-being.

bb) Use any personal information collected to estimate age or age range for any other purpose or retain that personal information longer than necessary to estimate age. (§ 1798.99.30(b).)

6) Establishes the California Children's Data Protection Working Group (CDPWG) within the Office of the Attorney General to deliver a report to the Legislature regarding best practices for the implementation of the AADC. (§ 1798.99.32.)

7) Subjects any business that violates the AADC to an injunction and 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, to be assessed and recovered in a civil action brought by the Attorney General. Allows for a 90-day notice-and-cure period in which a business may avoid liability under the AADC. Authorizes the AG to adopt regulations to clarify the requirements of the AADC. (§ 1798.99.35.)

8) Establishes the Digital Age Assurance Act, which requires a developer 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 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 the signal. (§ 1798.501(b).)

This bill:

1) Replicates many of the provisions of the AADC, as described below, in new code sections.

2) Requires a business that provides an online service, product, or feature likely to be accessed by children to take all of the following actions:
   a) Estimate 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 pursuant to subdivision (b) of Section 1798.501 or apply the privacy and data protections afforded to children to all consumers.

b) Configure all default privacy settings provided to children by the online service, product, or feature to settings that offer a high level of privacy.
c) Provide any privacy information, terms of service, policies, and community standards concisely, prominently, and using clear language suited to the age of children likely to access that online service, product, or feature.
d) If the online service, product, or feature allows the child's parent, guardian, or any other consumer to monitor the child's online activity or track the child's location, provide an obvious signal to the child when the child is being monitored or tracked.
e) Provide prominent, accessible, and responsive tools to help children, or if applicable their parents or guardians, exercise their privacy rights and report concerns.

3) Prohibits a business that provides an online service, product, or feature likely to be accessed by children from taking any of the following actions:
    a) Use the personal information of any child in a way that the business knows, or has reason to know, will cause an average child likely to access the online service, product, or feature either of the following harms:
        i. Significant mental suffering or distress that may, but does not necessarily, require medical or other professional treatment or counseling.
        ii. Discrimination against the child on the basis of race, ethnicity, sex, disability, sexual orientation, gender identity, gender expression, religion, or national origin.
    b) Profile a child by default.
    c) Collect, sell, share, or retain any personal information that is not necessary to provide an online service, product, or feature with which a child is actively and knowingly engaged, or as described in subparagraphs (A) to (D), inclusive, of paragraph (1) of subdivision (a) of Section 1798.145 of the Civil Code.
    d) If the end user is a child, use personal information for any reason other than a reason for which that personal information was collected.
    e) Collect, sell, or share any precise geolocation information of children by default unless the collection of that precise geolocation information is strictly necessary for the business to provide the service, product, or feature requested and then only for the limited time that the collection of precise geolocation information is necessary to provide the service, product, or feature.
    f) Collect any precise geolocation information of a child without providing an obvious sign to the child for the duration of that collection that precise geolocation information is being collected.

g) Use dark patterns to lead or encourage children to provide personal information beyond what is reasonably expected to provide that online service, product, or feature to forego privacy protections.
h) Use any personal information collected to estimate age or age range for any other purpose or retain that personal information longer than necessary to estimate age. Age assurance shall be proportionate to the risks and data practice of an online service, product, or feature.

4) Clarifies that nothing therein shall be construed to require a business to prevent or preclude a child from accessing or viewing any piece of media or category of media.

5) Provides for enforcement by the Attorney General and doubles the penalties that are provided for under the AADC.

6) Including a severability clause.

COMMENTS

1. Legal status of the AADC

The AADC was modeled after the Age Appropriate Design Code enacted in the United Kingdom. It instituted a series of obligations and restrictions on businesses that provide an online service, product, or feature likely to be accessed by a child ("covered business"). That term, "likely to be accessed by a child," means it is reasonable to expect, based on specified indicators, such as the nature of the content, the associated marketing, and the online context, that the online service, product, or feature would be accessed by children.

The AADC was almost immediately challenged on constitutional and federal preemption grounds by NetChoice, a tech trade association with members such as Google, Meta, OpenAI, TikTok, and Amazon. 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. In the preliminary injunction order, the federal district court acknowledged the goal of the AADC is to protect children when they are online and noted the unanimous support by California's legislature and Governor of the law. However, the Court concluded that the plaintiff "has shown that it is likely to succeed on the merits of its argument that the provisions of the CAADCA intended to achieve that purpose [protect children when online] do not pass constitutional muster." The Court examined at length Netchoice's First

Amendment claim and agreed that "[l]oss of free speech rights resulting from a threat of enforcement rather than actual enforcement constitutes irreparable harm."[2]

That initial ruling was appealed to the Ninth Circuit. That court upheld the preliminary injunction insofar as it enjoined enforcement of provisions relating to the DPIA:

> Although the district court stopped short of concluding that strict scrutiny governed its review of the DPIA report requirement, the court's ultimate conclusion that the DPIA report requirement is likely to fail First Amendment scrutiny was correct.
>
> Assuming arguendo that the State has a compelling interest in protecting children from "being pushed . . . unwanted material, such as videos promoting self-harm," as the State itself contends, the State is unlikely to show that the DPIA report requirement is "the least restrictive means" available for advancing that interest. As Amici American Civil Liberties Union and American Civil Liberties Union of Northern California (together, the ACLU) note in their amicus brief, the CAADCA's broad requirement that companies identify the risk of children being exposed to potentially harmful content necessarily compels companies to "assess the potential for [online] material to instigate grief, sorrow, pain, hurt, distress, or affliction in a minor." Such material
>
> > includes online mental health resources and communities that many children turn to for support. It touches reporting about school shootings, war, climate change, and teen suicide. And it reaches minors' own political or religious speech, as well as their personal updates about deaths in the family, rejection from a college, or a breakup.[3]

The Ninth Circuit panel found that the state could have "easily employed less restrictive means to accomplish its protective goals, such as by (1) incentivizing companies to offer voluntary content filters or application blockers, (2) educating children and parents on the importance of using such tools, and (3) relying on existing criminal laws that prohibit related unlawful conduct."[4]

The court also noted that "the relevant provisions are worded at such a high level of generality that they provide little help to businesses in identifying which of those practices or designs may actually harm children."[5] The court went on:

---

[2] *Netchoice, LLC v. Bonta* (N.D.Cal. 2023) 692 F. Supp. 3d 924.
[3] *NetChoice, LLC v. Bonta* (9th Cir. 2024) 113 F.4th 1101, 1121.
[4] *Ibid.*
[5] *Id.* at 1122.

> In addition, a disclosure regime that requires the forced creation and disclosure of highly subjective opinions about content-related harms to children is unnecessary for fostering a proactive environment in which companies, the State, and the general public work to protect children's safety online. For instance, the State could have developed a disclosure regime that defined data management practices and product designs without reference to whether children would be exposed to harmful or potentially harmful content or proxies for content. Instead, the State attempts to indirectly censor the material available to children online, by delegating the controversial question of what content may "harm to children" to the companies themselves, thereby raising further questions about the onerous DPIA report requirement's efficacy in achieving its goals. And while the State may be correct the DPIA reports' confidentiality reflect a degree of narrow tailoring by minimizing the burden of forcing businesses to speak on controversial issues, that feature may also cut against the DPIA report requirement's effectiveness at informing the greater public about how covered businesses use and exploit children's data.
>
> Ultimately, the DPIA report requirement falls well short of satisfying strict First Amendment scrutiny. The district court was therefore correct to conclude that NetChoice is likely to succeed in showing that the DPIA report requirement facially violates the First Amendment.[6]

Despite finding these provisions failed strict scrutiny, the Ninth Circuit sent the case back to the lower court to determine whether the DPIA provisions could be severed from the rest of the AADC.

On remand, the district court again blocked enforcement of the AADC.[7] The decision was again appealed to the Ninth Circuit. There, the court partially upheld and partially vacated the injunction.[8] The panel invalidated certain obligations, such as data use restrictions and dark patterns restrictions on the grounds that key statutory terms – "materially detrimental," "best interests" and "well-being" – were unconstitutionally vague. However, the court found Netchoice's challenge to the coverage definition failed as it did not take into consideration the entire scope of the definition – online products, services, and features likely to be accessed by children. The court removed the injunction on enforcement of this provision. The court also vacated the injunction as to the age estimation requirement and found the lower court inadequately assessed whether the notice-and-cure provision was severable from the AADC's remaining provisions. The Ninth Circuit instructed the lower court to more comprehensively

---

[6] *Ibid.*
[7] *NetChoice, LLC v. Bonta* (N.D.Cal. 2025) 770 F. Supp. 3d 1164.
[8] *NetChoice, LLC v. Bonta* (9th Cir. 2026) 170 F.4th 744.

assess the facts but affirmed the lower court's order enjoining enforcement of §§ 1798.99.31(b)(1)-(4) and 1798.99.31(b)(7).

2. Trimming the (unconstitutional) fat

This bill simply replicates the AADC in new code sections,[9] removing the various provisions or terms in the law that the Ninth Circuit has found unconstitutional, such as the DPIA requirements (and their attendant provisions) and the terms found unconstitutionally vague, such as "the best interests of the child" and "materially detrimental." The bill also omits the CDPWG provisions.

Last year, AB 1043 (Wicks, Ch. 675, Stats. 2025) established the Digital Age Assurance Act. That Act requires a developer 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 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 the signal. This bill reworks the age verification requirement of the AADC to align it with the Digital Age Assurance Act.

The bill also doubles the available civil penalties to $5,000 for negligent violations and $15,000 for intentional violations. It also includes a severability clause.

According to the author:

> As new technology continues to emerge and evolve, there needs to be comprehensive guardrails that protect children and their privacy while they are interacting and consuming content online. Providing more safeguards for children and their privacy is important because its misuse can expose children to harmful material, risks to their mental and physical health, and other challenges. AB 2246 would help make technology and online products safer for children and protect them from risks and features that may be harmful to them.

3. Stakeholder positions

Children Now, a sponsor of the bill, writes:

> Shortly after the AADC was signed into law by the Governor, an industry trade association sued to block its implementation, resulting in years of litigation. Recent rulings from the Ninth Circuit Court of Appeals (March

[9] Currently the bill creates a parallel, if narrowed, AADC in code. The author may wish to consider repealing the existing AADC to avoid any confusing overlap between the two statutes.

> 2026) have narrowed the scope of the legal dispute. While certain provisions—particularly those related to data protection impact assessments (DPIAs) and vague data-use restrictions—have been enjoined, the court upheld key structural elements of the law. Notably, the court found that the central "reasonably likely to be accessed by children" standard is likely constitutional on its face and upheld the age verification requirements. The ruling solidified the AADC as the most significant legislation to benefit and protect children since the enactment of the federal Children's Online Privacy Protection Act (COPPA) in 1994. It has turned the internet on its head and mandated that young people are able to navigate the internet safely in ways they have never been permitted.
>
> Since the enactment of the California AADC, at least a dozen states have followed with similar legislation. Many of those states have had the benefit of adapting their legislation to align with the findings of the Ninth Circuit Court of Appeals. With the introduction of AB 2246, California can also adapt its most expansive child online protection law to similarly withstand constitutional scrutiny and continue to lead the country in preventing harms stemming from online activities.

Several industry associations, including Technet, write jointly in opposition:

> We remain concerned about the bill's prohibition on profiling and personalization as a default for minor users, and in particular the absence of the safety valve that exists under the current AADC allowing companies to demonstrate that profiling is necessary to provide the service requested or that it is in the best interests of the child.
>
> Personalization is not simply a commercial feature — it is a critical tool that enables platforms to tailor experiences to individual users in ways that benefit teens and actively reduce their exposure to harmful or inappropriate content. Removing this capability as a default has real consequences:
>
> - Algorithmic filtering is a form of personalization that many platforms use to prevent harmful or borderline content from reaching minor users. Restricting this could make teens more, not less, likely to encounter age-inappropriate content. This is precisely the kind of safety tool parents want platforms to deploy.
> - Personalization helps teens connect with like-minded communities, including school friends, local religious organizations, and sports teams. A nonpersonalized experience undermines these connections and reduces the meaningful value these platforms offer young people.

> We respectfully request that this provision be amended to restore an exception
> consistent with the existing AADC, or alternatively that it be struck from the bill.

The American Academy of Pediatrics, California writes in support:

> Children and adolescents are among the most active internet users in the nation. According to national surveys, nearly all teenagers use online platforms daily, and many report online use almost constantly. At the same time, children often lack the developmental capacity to fully understand how their personal information is collected, shared, and monetized. Research consistently demonstrates that young users are less likely than adults to recognize sophisticated data collection practices, targeted advertising, behavioral profiling, and algorithmic tracking.
>
> These concerns are particularly significant because children's data can be used to build detailed behavioral profiles that persist for years. Academic studies examining online services used by children and adolescents have found evidence of extensive data sharing, tracking, and transmission of personal information to third parties, including advertising and marketing services, often before meaningful consent is obtained. Other research has identified shortcomings in age-specific privacy protections and found that online platforms do not always differentiate appropriately between child and adult users when collecting and processing personal data.

SUPPORT

Children Now (co-sponsor)
American Academy of Pediatrics, California
Bright Light Strategies
Los Angeles Unified School District
Project Liberty LLC

OPPOSITION

California Chamber of Commerce
Computer and Communications Industry Association
Technet

RELATED LEGISLATION

AB 2 (Lowenthal, 2026) 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 set to be heard in this Committee the same day as this bill.

AB 1709 (Lowenthal, 2026) prohibits online platforms that offer "addictive feeds" from allowing users under 16 years of age to create accounts. It requires these "covered platforms" to verify the age of users and implement reasonable measures to prevent users under 16 from accessing or using accounts on the platform. AB 1709 also creates an e-Safety Advisory Commission within the Department of Justice. AB 1709 is currently pending in this Committee.

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.

AB 2273 (Wicks, Ch. 320, Stats. 2022) *See* Executive Summary.

PRIOR VOTES:

Assembly Floor (Ayes 71, Noes 1)
Assembly Appropriations Committee (Ayes 13, Noes 0)
Assembly Judiciary Committee (Ayes 11, Noes 0)
Assembly Privacy and Consumer Protection Committee (Ayes 13, Noes 0)

****