
THIRD READING

Bill No: AB 2246
Author: Wicks (D), et al.
Amended: 4/23/26 in Assembly
Vote: 21

SENATE PRIV., DIGITAL TECH. & CONS. PROT. COMMITTEE: 8-0, 6/15/26

AYES: Cabaldon, Gonzalez, McNerney, Ochoa Bogh, Padilla, Reyes, Umberg,
Wiener

NO VOTE RECORDED: Jones

SENATE JUDICIARY COMMITTEE: 13-0, 6/30/26

AYES: Umberg, Niello, Allen, Ashby, Caballero, Durazo, Laird, Reyes, Stern,
Valladares, Wahab, Weber Pierson, Wiener

SENATE APPROPRIATIONS COMMITTEE: 7-0, 8/13/26

AYES: Cervantes, Seyarto, Cabaldon, Dahle, Grayson, Richardson, Wahab

ASSEMBLY FLOOR: 71-1, 5/26/26 - See last page for vote

SUBJECT: Online service, product, or feature: access by children

SOURCE: Children Now

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

ANALYSIS:

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. (Civil [Civ.] Code § 1798.99.28 et seq.)¹
- 3) Defines relevant terms within the AADC, including:
 - a) “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.
 - b) “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, 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:
 - a) 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.
 - b) Make DPIAs available to the Attorney General within 5 days of a request, as specified.
 - c) 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.
 - d) 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.
 - e) Configure all default privacy settings provided to children by the online service, product, or feature to settings that offer a high level of privacy,

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

unless the business can demonstrate a compelling reason that a different setting is in the best interests of children.

- f) 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.
 - g) 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.
 - h) Enforce published terms, policies, and community standards established by the business, including, but not limited to, privacy policies and those concerning children.
 - i) 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:
- a) 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.
 - b) 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.
 - 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, unless the business can demonstrate a compelling reason that doing so is in the best interests of children.
 - d) 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.

- 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, 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.
 - 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. (§ 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) Includes a severability clause.

Background

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. For a more thorough analysis of this bill, please see the Senate Privacy, Digital Technologies, and Consumer Protection Committee analysis.

Comments

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.

FISCAL EFFECT: Appropriation: No Fiscal Com.: Yes Local: No

According to the Senate Appropriations Committee:

Estimated \$840,000 in FY 2026-27, increasing to \$1.5 million annually to the Consumer Protection Section of the Department of Justice (DOJ) to conduct legal research, prepare documents for appeals, writs, trials and arbitration proceedings, including discovery, court appearances, and conducting complex and sensitive investigations. (Consumer Privacy Fund, General Fund)

Potentially significant costs to the courts to adjudicate civil actions. Expanding civil penalties could lead to lengthier and more complex court proceedings with attendant workload and resource costs to the court. While the courts are not funded on a workload basis, an increase in workload could result in delayed court services and would put pressure on the General Fund to fund additional staff and resources. The FY 2026-27 Budget appropriated \$70 million General Fund for this purpose (Trial Court Trust Fund, General Fund).

SUPPORT: (Verified 8/13/26)

Children Now (source)
American Academy of Pediatrics, California
Bright Light Strategies
California Academy of Child and Adolescent Psychiatry
Los Angeles Unified School District
Omidyar Network
Project Liberty LLC

OPPOSITION: (Verified 8/13/2026)

California Chamber of Commerce
Computer and Communications Industry Association
Technet

ARGUMENTS IN SUPPORT: Children Now writes:

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.

ARGUMENTS IN OPPOSITION: A group of industry associations, including Technet, writes:

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.

ASSEMBLY FLOOR: 71-1, 5/26/26

AYES: Addis, Aguiar-Curry, Ahrens, Alanis, Alvarez, Arambula, Ávila Farías, Bains, Bauer-Kahan, Bennett, Berman, Boerner, Bonta, Bryan, Calderon, Caloza, Carrillo, Castillo, Chen, Connolly, Davies, Dixon, Elhawary, Ellis, Flora, Fong, Gabriel, Gallagher, Garcia, Gipson, Mark González, Hadwick, Haney, Harabedian, Hart, Hoover, Irwin, Jackson, Kalra, Krell, Lee, Lowenthal, McKinnor, Nguyen, Ortega, Pacheco, Papan, Patel, Patterson, Pellerin, Petrie-Norris, Quirk-Silva, Ramos, Ransom, Michelle Rodriguez, Rogers, Blanca Rubio, Sanchez, Schiavo, Schultz, Sharp-Collins, Solache, Soria, Stefani, Valencia, Wallis, Ward, Wicks, Wilson, Zbur, Rivas

NOES: DeMaio

NO VOTE RECORDED: Jeff Gonzalez, Johnson, Lackey, Macedo, Muratsuchi, Celeste Rodriguez, Ta, Tangipa

Prepared by: Christian Kurpiewski / P., D.T., & C.P. / (916) 651-1548 / Benjamin Diaz/ P., D.T., & C.P. / (916) 651-1548
8/14/26 14:58:16

**** END ****