Date of Hearing: April 16, 2026
Fiscal: Yes

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
AB 2246 (Wicks) – As Amended April 6, 2026

PROPOSED AMENDMENTS

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

SYNOPSIS

In 2022, the Legislature, drawing on a similar law adopted in the United Kingdom, enacted the California Age-Appropriate Design Code Act (AADC), a bipartisan measure intended to protect the privacy, safety, and well-being of children when engaging with online products and services that children are likely to access. This Committee's analysis emphasized that the AADC is distinct from other federal and state efforts to protect children online because those statutes permit online platforms to treat all consumers as adults, unless there is actual knowledge that a consumer is a child, and therefore do not offer the highest privacy protections by design or default. The AADC inverted this scheme by instead requiring that if a platform is likely to be accessed by children, it should be safe for kids.

In broad strokes, the AADC requires covered businesses to perform data protection impact assessments (DPIA) and mitigate identified harms, estimate the age of users, and provide default privacy settings, among other protections. The law also prohibits businesses from using a child's personal information in a materially detrimental way, profiling the child, collecting and sharing more personal information than is necessary, collecting precise geolocation information, and using dark patterns. The AADC also provides for the creation of a Data Protection Working Group (DPWG) and is enforceable only by the Attorney General.

Shortly after the passage of the AADC, NetChoice, a trade association whose members include Google, Meta, and Amazon, initiated a litigation saga that continues to this day. Last month, however, the Ninth Circuit issued a decision that suggests that the bulk of the law's provisions may be constitutional or can be so by excising vague language. This bill broadly replicates the provisions of the AADC, other than those governing the DPWG, while omitting and recasting the portions that the Ninth Circuit has deemed unconstitutional – namely, the DPIA and related provisions, and vague language in the data use restriction, prohibition on profiling, data minimization, and dark patterns prohibition.

The bill is sponsored by Children Now and is supported by Tech Oversight California. TechNet, Computer & Communications Industry Association, and California Chamber of Commerce have a "concerns" position.

Amendments described in Comment #6 would align the age estimation provision with AB 1043 (Wicks; Ch. 675, Stats. 2025), augment civil penalties, and make other conforming changes.

Should the bill pass this Committee, it will next be referred to the Judiciary Committee.

EXISTING LAW:

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

2) Defines for purpose of the AADC key terms, 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:

        i. 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.).
        ii. 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.
        iii. An online service, product, or feature with advertisements marketed to children.
        iv. An online service, product, or feature that is substantially similar or the same as an online service, product, or feature subject to (ii).
        v. 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.
        vi. A significant amount of the audience of the online service, product, or feature is determined, based on internal company research, to be children.

    e. "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.)

3) Requires a business to provide 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. 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.

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, 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).)

4) 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).)

5) Establishes the California Children's Data Protection Working Group (DPWG) 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.)

6) Any business that violates the AADC is subject to an injunction and liable for a civil penalty of not more than two thousand five hundred dollars ($2,500) per affected child for each negligent violation or not more than seven thousand five hundred dollars ($7,500) per affected child for each intentional violation, to be assessed and recovered only in a civil action brought in the name of the people of the State of California 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.)

THIS BILL:

1) Broadly replicates the provisions of the AADC, other than the provisions governing the DPWG, while omitting the portions that the Ninth Circuit has deemed unconstitutional: data protection impact assessments and related provisions; and "materially detrimental" and "best interests" language in various provisions.

2) Provides that a business cannot 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:

    a. Significant mental suffering or distress that may, but does not necessarily, require medical or other professional treatment or counseling.

    b. Discrimination against the child on the basis of race, ethnicity, sex, disability, sexual orientation, gender identity, gender expression, religion, or national origin.

3) Omits the provision described above that requires a business to enforce published terms, policies, and community standards established by the business, including, but not limited to, privacy policies and those concerning children.

4) Includes a severability clause.

COMMENTS:

1) **Author's statement**. 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.

2) **The Age Appropriate Design Code**. In 2022, the Legislature, drawing on a similar law adopted in the United Kingdom, enacted the AADC to protect the privacy, safety, and well-being of children when engaging with online products and services that children are likely to access.[1] Key provisions are described below.

---

[1] § 1798.99.29

Coverage definition. The AADC applies to CCPA covered-businesses[2] that provide online services, products, or features "likely to be accessed by children" under age 18. A covered business is "likely to be accessed by children" when "it is reasonable to expect, based on [specified] indicators, that the online service, product, or feature would be accessed by children."[3] Such indicators include whether the platform is directed, routinely accessed by, advertises to, or has design elements known to be of interest to children.[4]

Requirements. The AADC requires covered businesses to do, among other things, the following:

- Data protection impact assessments: Conduct a systematic survey to identify and mitigate "any risk of material detriment to children that arises from the data management practices of the business"[5] including whether the design of the product, service, or feature could lead children to experience "potentially harmful" content, contacts, conduct, or whether algorithms, targeted advertising, engagement optimizing features, and processing sensitive information may harm children.[6] DPIAs were to be completed by July 1, 2024.

- Age estimation: Businesses must "[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, in the alternative, "apply the privacy and data protections afforded to children to all consumers."[7] Businesses are also prohibited from using personal information used to estimate age for any other purpose and retaining it longer than necessary to estimate age.[8]

- Default privacy settings: Configure all settings by default to "a high level of privacy," unless it can demonstrate that a different setting "is in the best interests of children."[9]

- Age-appropriate disclosures: Provide privacy information, terms of service, policies, and community standards in language suited to the age of children likely to access the service, product, or feature.[10]

- Parental monitoring/tracking signal for children: Provide an obvious signal to children when a parent, guardian, or other consumer monitors the child's online activity or tracks the child's location.[11]

- Policy enforcement: Enforce published terms, policies, and community standards established by the business, including, but not limited to, privacy policies and those concerning children.[12]

---

[2] Covered businesses are those that earn more than $25,000,000 annually or share at least 100,000 consumers' information annually. (§ 1798.140(d).) The AADC incorporates the CCPA's definitions. (§ 1798.99.30(a).)
[3] § 1798.99.30(b)(4).
[4] *Ibid*.
[5] § 1798.99.31(a)(2).
[6] § 1798.99.31(a)(1).
[7] § 1798.99.31(a)(5).
[8] § 1798.99.31(b)(8).
[9] § 1798.99.31(a)(6).
[10] § 1798.99.31(a)(7).
[11] § 1798.99.31(a)(8).
[12] § 1798.99.31(a)(9).

- Accessible tools: Provide prominent, accessible, and responsive tools to help children, or if applicable their parents or guardians, exercise their privacy rights and report concerns.[13]

Prohibitions. The AADC prohibits covered businesses from doing, among other things, the following:

- Data use restrictions: Using the child's personal information 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."[14]

- Profiling: Using automated processing of personal information to evaluate a child and predict preferences or behavior unless (1) the business can demonstrate it has "appropriate safeguards" and (2) profiling is necessary to provide service, product, or feature, or the business can demonstrate profiling is in the "best interests" of children."[15]

- Data minimization: Collecting, selling, sharing, retaining or using more personal information than is necessary, unless the business can demonstrate doing so is in the "best interests" of the child.[16]

- Precise geolocation protections: Collecting precise geolocation information of a child unless it is "strictly necessary" and an obvious sign is provided to the child.[17]

- Dark patterns: Using techniques that encourage children to provide more personal information than is necessary 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."[18]

Children's Data Protection Working Group. The AADC provides for the creation of a working group in the AG's Office to deliver a report regarding best practices for implementing the act. The working group consists of appointees from the Governor, Legislature, AG, and Privacy Agency. Subjects of the report include identifying covered businesses, evaluating and prioritizing the best interests of children, implementing age assurance, assessing and mitigating risks, publishing age-appropriate disclosures, and leveraging the expertise of the Privacy Agency.[19]

Enforcement and notice-and-cure provision. The AG has authority to enforce the AADC. Id. § 1798.99.35(a). Violators face civil penalties of up to $2,500 per child for each negligent violation and up to $7,500 for each intentional violation. The law contains a provision that

---

[13] § 1798.99.31(a)(10).
[14] § 1798.99.31(b)(1).
[15] § 1798.99.31(b)(2).
[16] § 1798.99.31(b)(3), (4).
[17] § 1798.99.31(b)(5), (6).
[18] § 1798.99.31(b)(7).
[19] § 1798.99.32.

allows businesses to cure an alleged violation with respect to DPIA requirements within 90 days of written notice from the Attorney General of the alleged violation.[20]

3) **Litigation saga**. The AADC was challenged by NetChoice, a trade association representing major tech companies, including Meta, Google, Amazon, and Netflix. The case has twice been heard by the District Court for the Northern District of California and twice appealed to a three-judge panel of the Ninth Circuit Court of Appeals, which recently issued a decision partially overruling the lower court and remanding the case for a third set of proceedings. To understand the current state of the law, which is partially blocked pending those proceedings, this section highlights the two Ninth Circuit panel decisions.

NetChoice v. Bonta, Part I (2024): *DPIA provisions blocked on First Amendment grounds.* Following the Northern District's ruling that blocked enforcement of the AADC on First Amendment grounds,[21] the Ninth Circuit panel upheld the block on the DPIA requirement, along with related provisions, including the notice-and-cure provision.[22] The panel found that compelling platforms to identify harmful content, document it, and publish the assessments constitutes content-specific compelled speech on a matter of public controversy, as opposed to commercial speech (advertisements, labels, etc.). As a result, the DPIA requirement triggered the most exacting form of judicial review known as "strict scrutiny," which requires the government to show the speech restriction is narrowly tailored to serve a compelling interest and does so by the least restrictive means. The panel noted that "potentially harmful content" swept in mental health support communities, school shooting coverage, climate reporting, and teenagers' own posts about grief and rejection. The panel concluded that less restrictive alternatives like parentally-controlled content filters and parental educational tools exist, and the State of California had not shown why they were inadequate. The panel sent the case back to the lower court to determine whether the DPIA provisions could be severed from the rest of the AADC.[23]

NetChoice v. Bonta, Part II (March 2026): *Data use restrictions and dark patterns prohibitions blocked on vagueness grounds; coverage and age estimation unblocked.* After the lower court once again blocked enforcement of the AADC,[24] the case returned to the same panel of the Ninth Circuit. The panel issued a mixed ruling, upholding the block on the law for some provisions while holding that others could go into effect pending further proceedings.

First, with respect to the AADC's coverage definition – online products, services, and features likely to be accessed by children – the panel ruled that NetChoice had failed to show that the provision is unconstitutional on its face. A facial challenge seeks to strike down a law in all its applications (as opposed to asserting that the law, as applied to a particular case, is unconstitutional) by showing that the law's unconstitutional applications substantially outweigh constitutional ones. NetChoice failed to make this showing because it only submitted evidence relating to social media companies, while the law's scope broadly encompasses a range of businesses like ridesharing, ticketing, and financial services. Concluding the coverage definition

---

[20] § 1798.99.35.
[21] *Netchoice, LLC v. Bonta* (N.D.Cal. 2023) 692 F. Supp. 3d 924, 936.
[22] *NetChoice, LLC v. Bonta* (9th Cir. 2024) 113 F.4th 1101, 1125 (*NetChoice I)*.
[23] See *NetChoice I*, *supra,* 113 F.4th at 1123-24.
[24] *NetChoice, LLC v. Bonta* (N.D.Cal. 2025) 770 F. Supp. 3d 1164, 1177.

was "likely constitutional," the panel lifted the block on enforcement of this provision and ordered the lower court to address this issue more comprehensively.[25]

Second, the panel also found that the evidentiary record was underdeveloped on whether the age estimation provision actually burdens protected speech. Covered businesses can opt out of this requirement entirely by defaulting to child-level privacy protections for all users, a fact that the lower court had not properly considered. The court lifted the block on the age estimation provision and ordered the lower court to address the issue more comprehensively.[26]

Third, the panel affirmed the lower court's block on the data use restrictions and dark patterns prohibitions on vagueness grounds. The panel agreed that terms like "materially detrimental," "well-being," and "best interests of children" provide insufficient guidance to businesses about what conduct is prohibited. As the panel noted, "best interests" is a concept imported from family law in which judges make considered decisions on a case-by-case basis – a task for which businesses are ill-equipped.[27] With respect to the "materially detrimental" standard, the panel observed that "the range of harms that could plausibly qualify as 'materially detrimental' is vast, spanning everything from financial exploitation to sleep loss, distraction, or hurt feelings."[28]

Finally, the panel vacated the district court's determination that the notice-and-cure provision was not "volitionally" severable from the AADC's valid remainder. An invalid statutory provision may be severed if it is "grammatically, functionally, and volitionally severable."[29] A provision is volitionally severable if the remainder would not have been adopted by the Legislature in its absence. Finding the record underdeveloped on whether the Legislature considered the notice-and-cure provision – which was added on the Senate floor, along with other substantive changes, shortly before both houses passed the bill with zero "no" votes – necessary to the AADC's passage, the panel ordered the lower court to address this issue more comprehensively.[30]

The current status of the AADC's provisions is summarized in the table below.

Provision	**Status**
DPIA report, mitigation requirements, and dependent provisions, including the notice-and-cure provision	**Blocked**; lower court's ruling on this provision upheld in *NetChoice I* on First Amendment grounds as content-specific compelled noncommercial speech.
Data use restriction, prohibition on profiling, data minimization, dark patterns prohibition	**Blocked**; lower court's ruling on these provisions upheld in *NetChoice II* on vagueness grounds; undefined terms phrases like "materially detrimental to well-being" and "best interests" were so broad they failed to provide companies with sufficient guidance to

[25] *Netchoice, LLC v. Bonta* (9th Cir. Mar. 12, 2026, No. 25-2366) 2026 LX 177668, at *29. (*NetChoice II.*)
[26] *Id.* at *36.
[27] *Id.* at *42.
[28] *Id.* at *46.
[29] *California Redevelopment Assn. v. Matosantos* (2011) 53 Cal.4th 231, 271.
[30] *NetChoice II, supra,* LX 177668 at *54.

	comply.
Coverage definition	**Operative**; lower court's block lifted in *NetChoice II*, subject to further proceedings based on impact to entities other than social media companies.
Age estimation	**Operative**; lower court's block lifted in *NetChoice II*, subject to further proceedings based on whether protected speech is burdened even if a business opts out of age estimation by applying child-level privacy protections to all users.
Age-appropriate transparency, policy enforcement, accessible tools, default privacy settings, precise geolocation protections, age-appropriate privacy disclosures, Children's Data Protection Working Group, enforcement (other than the notice-and-cure provision)	**Operative**; lower court's block lifted in *NetChoice II*, subject to further proceedings including a potential finding by the district court that the Legislature would not have passed the AADC without the notice-and-cure provision.

4) **This bill excises the unconstitutional provisions of the AADC**. This bill broadly replicates the provisions of the AADC, other than those governing the DPWG, while omitting and recasting the portions that the Ninth Circuit has deemed unconstitutional – namely, the DPIA and related provisions, and the vague "materially detrimental" and "best interests" language in the data use restriction, prohibition on profiling, data minimization, and dark patterns prohibition. The bill omits the provision requiring businesses to enforce their own policies. And the data use restriction has been recast to instead provide that a business cannot use the personal information of the average child likely to access the platform, product, or service in a way that the business knows or has reason to know will cause the child to experience significant mental suffering or distress or discrimination on the basis of a protected characteristic.

The omission of the offending provisions does not itself render the bill constitutional. Rather, excising those provisions means the bill is *not* unconstitutional on issues that have been settled in the ongoing litigation saga described above – although there are some strong indications that further challenges against many of the provisions are unlikely to succeed. Going forward, the author may wish to continue refining the language or adding additional definitions of key terms to protect the bill against litigation. Additionally, the author may wish to consider whether the current provisions of the AADC, other than the section establishing the DPWG, should be deleted to avoid overlapping schemes.

5) **Concerns**. TechNet, Computer & Communications Industry Association, and California Chamber of Commerce jointly write:

> We want to highlight a couple of initial concerns for consideration. First, AB 2246 doesn't appear to take into account the numerous bills that have passed since the Age Appropriate Design Code (AADC) passed in 2022. California has enacted 23 laws related

to online safety since then including SB 976 (2024), SB 243 (2025), AB 56 (2025), and AB 1043 (2025), not to mention the dozens of proposals being considered this year alone. This is all in addition to the significant protections afforded users of all ages by the California Consumer Privacy Act (CCPA). Moreover, rather than amend the existing AADC, AB 2246 would create a new law in a different section of the California code. If AB 2246 were to pass in its current form, the end result would be two laws in place with similar—though not identical—requirements. It is crucial that all of these laws are consistent and minimize overlapping requirements to the greatest extent possible.

Second, it appears that AB 2246 is perhaps intended to respond to judicial findings as part of the ongoing litigation over the AADC. It is important to note that, from a procedural standpoint, the findings to date in this case are preliminary. We thus encourage the legislature allow the judicial process to run its course and await conclusive decisions on the AADC before beginning to amend the law's substantive terms.

Third, a couple of changes warrant further review and discussion to minimize unintended consequences. In particular, the prohibition against profiling by default excludes the exception under the AADC for companies to demonstrate that proper safeguards have been put in place, that profiling is necessary to provide the service requested or that it is in the best interests of the child. Profiling is often used to help provide a consistent, safe, and age-appropriate experience online. Furthermore, AB 2246 prohibits companies from using a minor's personal information in any way that the business knows or should reasonably know will cause an average child to suffer significant mental suffering, distress or discrimination on the basis of a protected class. Apart from the obvious intent of protecting children, it's not clear what harms or business actions this section is trying to prevent, particularly since discrimination may be duplicative of the Unruh Civil Rights Act.

6) **Amendments.** The author has agreed to amend the bill to do the following:

- Update the age estimation provision to align with AB 1043 (Wicks; Ch. 675, Stats. 2025), which establishes a device-based age-verification system.
- Omit the "best interests" clause in the default privacy setting provision.
- Double the amount of the civil penalties.

ARGUMENTS IN SUPPORT: Children Now, the bill's sponsor, 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 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 CA 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 CA AADC, at least another 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 2243, 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.

Tech Oversight California writes:

Proof young people need better protections couldn't be more conclusive: in the span of 24 hours last month, juries in California and New Mexico delivered the first monetary verdicts in American history holding social media companies liable for design-driven harm to young users. TOC worked closely on the Los Angeles bellwether case, in which a jury found Meta and Google liable for designing platforms whose addictive features -- algorithmic amplification, infinite scroll, social comparison mechanics -- caused lasting psychological harm to a young woman who began using these products as a child. The day before, a New Mexico jury ordered Meta to pay $375 million in civil penalties for misleading the public about platform safety and enabling child sexual exploitation.

These verdicts confirm what parents and advocates have known for years: the harms are rooted in product design, and design-centered solutions are exactly the right response. The Los Angeles case was the first bellwether in litigation involving thousands of plaintiffs – families, school districts, states, and localities – with additional trials scheduled through 2026 and beyond, continuing to shine a spotlight on the severity of this problem and the urgency to act.

The 9th Circuit has clarified the path forward. The court's March 12, 2026 ruling in NetChoice v. Bonta rejected the industry's attempt to strike down the AADC in its entirety. The court found that NetChoice failed to show the law's coverage definition or age estimation requirement facially violates the First Amendment. It also identified with precision the provisions that need tightening on vagueness grounds. AB 2246 incorporates those lessons directly, with statutory language designed to be clear and concise to withstand future constitutional challenges from Big Tech.

The threat is evolving, and the legislation must evolve with it. The scope and severity of the AI chatbot problem has grown dramatically since the original AADC was enacted. Multiple lawsuits against Character.AI -- including cases tied to the deaths of children who formed destructive emotional attachments to AI companions -- resulted in settlements earlier this year. A separate lawsuit against OpenAI over the death of California teenager Adam Raine is ongoing. These cases have exposed a category of design-driven harm that did not exist at scale in 2022: products that create the illusion of talking with a human being and deliberately elicit feelings of intimacy from young users, often with devastating consequences.

Because the Kids Code approach is purposely platform-neutral, the AADC laws already

going into effect in other states offer some of the first protections in the country for kids interacting with AI. AB 2246 offers us the opportunity to go further by incorporating new legislative language that more directly addresses chatbot-specific risks, including expanding covered design features to capture an even wider array of online products and services. We can continue to build on design-centered solutions to design-centered problems, and place responsibility where it belongs: on the companies that build these products and profit from our kids' engagement.

We have been honored to work alongside families affected by these harms to amplify their stories and seek the design-centered reforms that these cases prove are necessary. We applaud your continued leadership in this space and look forward to working with you to ensure California continues to lead the country in the protection of kids online.

REGISTERED SUPPORT / OPPOSITION:

Support

Children Now (Co-Sponsor)
Tech Oversight CA (Co-Sponsor)

Opposition

California Chamber of Commerce
Computer and Communications Industry Association
Technet

Analysis Prepared by: Josh Tosney / P. & C.P. / (916) 319-2200