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

AB 2246 (Wicks)
Version: April 23, 2026
Hearing Date: June 30, 2026
Fiscal: Yes
Urgency: No
AWM

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

In 2022, the Legislature enacted AB 2273 (Wicks, Ch. 320, Stats. 2022), which established the AADC. The AADC places a series of obligations and restrictions on businesses that provide online services, products, or features likely to be accessed by children, including 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 AADC also requires specified businesses to perform data protection impact assessments (DPIA) and to provide default privacy settings and other protections. Additionally, the AADC calls for the creation of a Children's Data Protection Working Group (CDPWG) tasked with delivering a report on best practices for AADC implementation.

The AADC was challenged in court by NetChoice, a trade group representing most of the major social media platforms, shortly after going into effect. Portions of the AADC have been enjoined, including the creation of the CDPWG, but large portions of the AADC remain in effect. The case is ongoing. (*See NetChoice LLC v. Bonta* (N.D. Cal.) Case No. 22-cv-08861-BLF.)

This bill replicates, in different code sections, the portions of the AADC that have not been enjoined, and further narrows certain provisions in order to ensure their constitutionality.

This bill is sponsored by Children Now and is supported by the American Academy of Pediatrics, the California Academy of Child and Adolescent Psychiatry, Common Sense Media, the Los Angeles Unified School District, and the Omidyar Network. This bill is opposed by the California Chamber of Commerce, the Computer Communications Industry Association, and TechNet. The Senate Privacy, Digital Technologies, and Consumer Protection Committee passed this bill with a vote of 8-0.

PROPOSED CHANGES TO THE LAW

Existing constitutional law:

1) Provides that Congress shall make no law abridging the freedom of speech. (U.S. Const., 1st amend. (the First Amendment) & 14th amend.; *see Gitlow v. People of State of New York* (1925) 268 U.S. 652, 666 (First Amendment guarantees apply to the states through the due process clause of the Fourteenth Amendment).)

2) Provides that every person may freely speak, write, and publish their sentiments on all subjects, and that a law may not restrain or abridge liberty of speech. (Cal. Const., art. I, § 2.)

Existing federal law 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.)

Existing state law:

1) Establishes the AADC. (Civ. Code, div. 3, pt. 4, tit. 1.81.47, §§ 1798.99.28 et seq.)[1]

2) 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:

[1] This portion of the analysis sets forth the text of the AADC as it is currently in statute; the portions which have been preliminarily enjoined are discussed in Comment 2, below.

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

3) 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. 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. (Civ. Code, § 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. (Civ. Code, § 1798.99.30(b).)

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

6) 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.
    a) The bill provides a 90-day notice-and-cure period in which a business may avoid liability under the AADC.
    b) The Attorney General may adopt regulations to clarify the requirements of the AADC. (Civ. Code, § 1798.99.35.)

7) Establishes the Digital Age Assurance Act (DAAA), 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. (Civ. Code, div. 3, pt. 4, tit. 1.81.9, §§ 1798.500 et seq.)

This bill:

1) Sets forth the same definitions as in the AADC, except "data protection impact assessment" is not defined because there is no DPIA included in this bill.

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 the DAAA 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 or 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) Using the personal information of any child in any 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 the child is actively and knowingly engaged, or as described in the California Consumer Privacy Act (CCPA).
    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 the age or age range for any other purpose or retain that personal information longer than necessary to estimate age; age assurance shall be proportional to the risks and data practice of an online service, product, or feature.

4) Provides that nothing in 2) or 3) shall be construed to require a business to prevent or preclude a child from accessing or viewing any piece of media or a category of media.

5) Provides that any business that violates this bill's requirements shall be subject to an injunction and liable for a civil penalty of not more than $5,000 per affected child for each negligent violation, or not more than $15,000 per affected child for each intentional violation, which shall 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.

6) Provides that any penalties, fees, and expenses recovered in an action under 5) shall be deposited in the Consumer Privacy Fund within the General Fund with the intent that they be used to fully offset costs incurred by the Attorney General in connection with this bill.

7) Provides that nothing in this bill shall be interpreted to serve as the basis for a private right of action under the bill or any other law.

8) Permits the Attorney General to solicit broad public participation and adopt regulations to clarify the bill's requirements.

9) Provides that the bill does not apply to information or entities exempt from the CCPA, as specified.

10) Includes a severability clause.

COMMENTS

1. Author's comment

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. Background on the AADC and its legal status

In 2022, the Legislature enacted AB 2273 (Wicks, Ch. 320, Stats. 2022), which established the AADC. According to the Senate Privacy, Digital Technologies, and Consumer Protection Committee's analysis of this bill, the AADC was modeled after the British Age Appropriate Design Code. The AADC imposes a number of obligations on businesses with online services or platforms "likely to be accessed by a child," including performing a DPIA for any new online service to be offered to the public; documenting whether certain practices result in harm to a child; and estimating the age of child users with reasonable certainty and configuring privacy settings accordingly. The bill was enforceable only by the Attorney General.[2]

NetChoice, an internet trade group "whose members consist of large technology companies like Amazon, Google, Meta, and Netflix" sued to challenge the AADC on constitutional grounds before it even took effect and sought a preliminary injunction to prevent the AADC's enforcement.[3] The district court agreed with NetChoice and enjoined the AADC in full, and California appealed.[4]

While that appeal was pending, the United States Supreme Court issued *Moody v. NetChoice*, which clarified the legal standard for a facial challenge under the First Amendment.[5] The thrust of that opinion was that lower courts were treating "as-applied [First Amendment] claims more like facial ones" and, as a result, improperly enjoining laws without "address[ing] the full range of activities the laws cover, [or] measur[ing] the constitutional claims against the unconstitutional applications."[6]

---

[2] Civ. Code, § 1798.99.35.
[3] *NetChoice, LLC v. Bonta* (9th Cir. 2026) 170 F.4th 744, 751-752 (*NetChoice II*).
[4] *Id.* at p. 752.
[5] *See Moody v. NetChoice LLC* (2024) 603 U.S. 707, 723.
[6] *Id.* at p. 724.

Fresh off of the Supreme Court's judicial scolding, the Ninth Circuit affirmed the district court's injunction in part and remanded the case for further proceedings, in which the district court was instructed to apply the standard for facial challenges articulated in *Moody* and to determine whether the unconstitutional parts of the AADC could be severed from the constitutional parts.[7] On remand, NetChoice asserted additional First Amendment challenges to the AADC.[8] The district court analyzed NetChoice's claims under the strict scrutiny test and again enjoined large portions of the AADC.[9] California again appealed. The Ninth Circuit again agreed with the district court in part and reversed in part.[10] In reversing parts of the district court's injunction order, the Ninth Circuit relied heavily on *Moody* to hold that NetChoice had not carried its burden to succeed on a facial challenge.[11]

The provisions of the AADC that are currently enjoined are:

- The DPIA requirement and provisions related to the DPIA.
- Some of the prohibitions on the use of a child's personal information by a business with an online service or product, including:
    - Use of a child's information in a way that a business knows, or has reason to know, is materially detrimental to the physical health, mental health, or wellbeing of a child.
    - Profiling a child.
    - Collecting, selling, sharing, or retaining a child's personal information that is not necessary to provide the online service or product, as specified.
    - Using a child user's personal information for any reason other than the reason for which the information was collected, as specified.
    - Using dark patterns to lead or encourage children to provide more information than reasonably expected to provide the service, as specified.[12]

After its second decision, the Ninth Circuit remanded the case to the district court for further proceedings, including for further development of the facts to determine whether NetChoice's First Amendment claims have merit. The case is ongoing.

3. <u>The new and improved AADC</u>

Although the district court has not fully ruled on NetChoice's challenge, this bill applies the courts' past guidance to implement a version of the AADC without the enjoined provisions and with additional changes to avoid First Amendment pitfalls. Unlike the original AADC, this bill does not include a DPIA requirement or require the creation of

---

[7] *NetChoice, LLC v. Bonta* (9th Cir. 2024) 113 F.4th 1101, 1108 (*NetChoice I*).
[8] *NetChoice II*, *supra*, 170 F.4th at p. 752.
[9] *Ibid.*
[10] *Id.* at p. 751.
[11] *Id.* at pp. 755, 760, 761.
[12] *NetChoice I*, *supra*, 113 F.4th at p. 1125; *NetChoice II*, *supra*, 170 F.4th at p. 770.

a working group to address children's data protection.[13] Instead, the bill merely imposes obligations and restrictions on businesses that offer an online product, service, or feature that is likely to be accessed by children.

Additionally, this bill incorporates a different age verification than the one in the original AADC. Last year, AB 1043 (Wicks, Ch. 675, Stats. 2025) established 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.

Finally, the bill increases the civil penalties that were available under the original AADC: for a negligent violation, $5,000 per violation instead of $2,500; and for an intentional violation, $15,000 instead of $7,500. The bill is still enforceable only by the Attorney General.

The Senate Privacy, Digital Technologies, and Consumer Protection Committee considered this bill from an overall policy standpoint and passed it with a vote of 8-0. This analysis focuses on the constitutional issues presented by the bill, discussed below.

4. Constitutional issues

As discussed in Comment 2, the Ninth Circuit affirmed the district court's injunction to the extent that it enjoined some of the obligations and restrictions relating to a child user's data. The Ninth Circuit based its decision on the "void for vagueness" doctrine, which "requires the invalidation of laws that are impermissibly vague."[14]

None of this bill's language replicates, word-for-word, currently enjoined provisions of the AADC. The bill does, however, use language similar to some of the enjoined provisions, with the apparent intention of achieving the same result. These include:

- The original AADC prohibited the use of a 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 wellbeing of a child. This bill prohibits the use of a child's personal information 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 significant mental distress or discrimination against the child on specified bases.

[13] The Ninth Circuit's most recent AADC decision vacated the district court's order enjoining the working group statute, so it's not clear that the current AADC statute can't go into effect. (*See NetChoice II*, *supra*, 170 F.4th at p. 770.)
[14] *Id.* at p. 763 (internal quotation marks omitted).

- The original AADC prohibited a business from profiling a child unless specific criteria were met, including that the business could demonstrate a compelling reason that profiling is in the best interests of children. This bill straightforwardly prohibits profiling a child.
- The original AADC prohibited collecting, selling, sharing, or retaining a child's personal information not necessary to provide the online service, unless the business can demonstrate that doing so was in the best interests of children likely to access the service. This bill prevents these data practices where they are not necessary to provide the online service, product, or feature with which a child is actively and knowingly engaged, or for purposes exempted from the CCPA.
- The original AADC prohibited, where the end user is a child, the use of their personal information for any reason other than the reason for which it was collected, unless the business can demonstrate that the use is in the best interests of children. This bill simply prohibits uses other than the reason for which it was collected.
- The original AADC prohibited the use of dark patterns to lead children to take actions that the business knows, or has reason to know, is materially detrimental to the child's physical health, mental health, or wellbeing. This bill prohibits a business from using dark patterns to lead or encourage children to provide personal information beyond what is reasonably expected or to forego privacy protections.

The bill's changes excise the concepts that the court found unconstitutionally vague, particularly the "best interests" standard.[15] The bill's opponents argue that some of the bill's terms remain vague, however. According to the bill's opponents:

> [T]he bill's prohibition on using personal information in ways that cause an "average child" to suffer "significant mental suffering, distress or discrimination on the basis of a protected class" raises ongoing concerns about vagueness. The Ninth Circuit recently found the term "mental suffering and distress" to be unconstitutionally vague in a related context. Apart from the clear intent to protect children, it is not clear what specific harms or business practices this provision is designed to prevent. The reference to discrimination may also be duplicative of the Unruh Civil Rights Act.

Additionally, because the lawsuit involving the original AADC is ongoing, it is possible that provisions of the original AADC, and this one, could be found unconstitutional as part of the pending as-applied challenge or after the development of facts to support the facial challenge. That is, however, a question for the courts, and there does not appear to be any harm in recodifying those existing provisions.

---

[15] *See id.* at pp. 764-767.

5. Arguments in support

According to the American Academy of Pediatrics:

> Strengthening protections against secondary uses of children's data is especially important given growing evidence that digital platforms continue to collect and leverage extensive information about young users. Recent federal enforcement actions have alleged that major social media companies collected data from children without appropriate consent and failed to adequately protect children's privacy rights. These cases underscore the need for strong state-level safeguards that prioritize children's well-being over commercial interests.
>
> AB 2246 will help ensure that California's privacy framework reflects a simple and commonsense principle: information collected from children should be used only for the purpose for which it was collected unless a parent or guardian affirmatively authorizes otherwise. By narrowing opportunities for misuse of children's data, the bill will reduce risks associated with profiling, targeted advertising, behavioral manipulation, and long-term digital surveillance.
>
> At a time when parents, educators, pediatricians, and youth advocates are increasingly concerned about the effects of pervasive digital tracking on children's health, safety, and development, California should continue to lead the nation in establishing strong, enforceable protections for young people online.

6. Arguments in opposition

According to the California Chamber of Commerce, the Computer & Communications Industry Association, and TechNet:

> As we noted in our earlier correspondence with the Assembly Committee on Privacy, we want to flag the broader legislative landscape as important context. California has enacted 23 laws related to online safety since the Age-Appropriate Design Code (AADC) passed in 2022, including SB 976 (2024), SB 243 (2025), AB 56 (2025), and AB 1043 (2025), in addition to the significant protections the California Consumer Privacy Act (CCPA) provides for users of all ages. AB 2246, rather than amending the existing AADC, would create a new law in a different section of the California code. If passed in its current form, the result would be two laws with similar — though not identical — requirements. It is essential that all of these laws are consistent and minimize overlapping requirements to the greatest extent possible…
>
> 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.

SUPPORT

Children Now (sponsor)
American Academy of Pediatrics
California Academy of Child and Adolescent Psychiatry
Common Sense Media
Los Angeles Unified School District
Omidyar Network

OPPOSITION

California Chamber of Commerce
Computer & Communications Industry Association
TechNet

RELATED LEGISLATION

Pending 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 pending before this Committee and is set to be heard on the same date 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 pending before this Committee and is set to be heard on the same date as this bill.

Prior legislation:

AB 1043 (Wicks, Ch. 675, Stats. 2025) is discussed in Comment 3 of this analysis.

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.

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

PRIOR VOTES

Senate Privacy, Digital Technologies, and Consumer Protection Committee (Ayes 8, Noes 0)
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)

****