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

AB 2007 (Bauer-Kahan)
Version: June 15, 2026
Hearing Date: June 23, 2026
Fiscal: No
Urgency: No
AWM

SUBJECT

Youth programs: identifying information of youth

DIGEST

This bill requires youth-focused programs, such as extracurricular and after-school programs, to obtain parental consent before using images of a child or other protected information in their communications, marketing, educational, or training materials, as specified.

EXECUTIVE SUMMARY

Parents and guardians are becoming increasingly concerned with their children's digital footprints. An innocently posted photo or video of a child, without privacy protections, can be used for a host of nefarious purposes, such the creation of deepfake materials, identity theft, and training AI. Many parents and guardians want to protect their children from these consequences, but not at the expense of participation in youth-focused programming, like sports leagues, camps, or other recreation activities. According to the author, however, some youth-focused programs are apathetic, or downright hostile, to parents' and guardians' requests that the program not use their child's personal information in the program's public-facing materials.

To provide parents with greater control over the use of their child's image, this bill requires organizations that offer youth-serving programming to provide a parent or guardian with a stand-alone release document that details specifically how and where a youth's information is intended to be used, and that the parent or guardian may revoke their consent at any time. Additionally, this bill prohibits organizations from making participation in programming contingent on a parent or guardian waiving their child's privacy rights and prohibits the organization from sharing or selling the child's covered information. The bill creates a private right of action against a covered entity that violates the bill's requirements, which may be brought by the parent or guardian of the child whose image or information was used without consent. The author has agreed to

a number of amendments to respond to stakeholder concerns; due to the timing of the hearings, these amendments will be taken in the Senate Privacy, Digital Technologies, and Consumer Protection Committee.

This bill is sponsored by the author and is supported by the California Catholic Conference. Although the Committee has not received formal opposition to the bill, the Committee has received a letter of concern from the California League of Cities and the California Park & Recreation Society. If this Committee passes this bill, it will be referred to the Senate Privacy, Digital Technologies, and Consumer Protection Committee.

PROPOSED CHANGES TO THE LAW

Existing constitutional law provides that all people are, by nature, free and independent and have inalienable rights, including the fundamental right to privacy. (Cal. Const., art. I, § 1.)

Existing state law:

1) States that the "right to privacy is a personal and fundamental right protected by Section 1 of Article I of the Constitution of California and by the United States Constitution and that all individuals have a right of privacy in information pertaining to them," and that the Legislature finds all of the following:
    a) The right to privacy is being threatened by the indiscriminate collection, maintenance, and dissemination of personal information and the lack of effective laws and legal remedies.
    b) The increasing use of computers and other sophisticated information technology has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information.
    c) In order to protect the privacy of individuals, it is necessary that the maintenance and dissemination of personal information be subject to strict limits. (Civ. Code, § 1798.1.)

2) Establishes the California Consumer Privacy Act (CCPA), which grants consumers certain rights with regard to businesses' collection of their personal information, including enhanced notice, access, and disclosure; the right to deletion; the right to restrict the sale of information; and protection from discrimination for exercising these rights. It places attendant obligations on businesses to respect those rights. (Civ. Code, div. 3, pt. 4, tit. 1.81.5, §§ 1798.100 et seq.)

3) Defines "personal information" within the CCPA as information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably linked, directly, or indirectly, with a particular consumer or household, including the following:

a) Identifiers such as a real name, postal address, unique personal identifier, online identifier, IP address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.
b) Characteristics of protected classifications under California or federal law.
c) Commercial information, including property records and records of purchases.
d) Biometric information.
e) Internet or other electronic network activity information, including browser and search history.
f) Geolocation data.
g) Audio, electronic, visual, thermal, olfactory, or similar information. (Civ. Code, § 1798.140(v)(1).)

4) Excludes, from the definition of "personal information" within the CCPA:
   a) Publicly available information or lawfully obtained, truthful information that is a matter of public concern.
   b) Deidentified or aggregate consumer information. (Civ. Code, § 1798.140(v)(2) & (3).)

5) Prohibits a business from selling or sharing the personal information of a consumer if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of those who are between 13 and 16 years of age, or the consumer's parent or guardian, in the case of a consumer who is less than 13 years of age, has affirmatively authorized the sale or sharing of the information. (Civ. Code, § 1798.120.)

6) Provides that any person who knowingly uses another's name, voice, signature, photograph, or likeness, in any manner, on or in products, merchandise, or goods, or for purposes of advertising or selling, or soliciting purchases of, products, merchandise, goods, or services, without that person's prior consent, or, in the case of a minor, the prior consent of their parent or guardian, shall be liable for the following:
   a) Statutory damages of $750 per violation or the actual damages suffered by the person, whichever is greater.
   b) Any profits from the unauthorized use that are attributable to the use and are not taken into account in computing the actual damages.
   c) Punitive damages.
   d) Attorney's fees and costs. (Civ. Code, § 3344(a).)

7) Provides that the use of a name, voice, signature, photograph, or likeness in a commercial medium shall not constitute a use for which consent is required under 6) solely because the material containing the use is commercially sponsored or contains paid advertising; rather, it shall be a question of fact as to whether or not the use of

the name, voice, signature, photograph, or likeness was so directly connected with the commercial sponsorship or with the paid advertising as to constitute a use for which consent is required under 6). (Civ. Code, § 3344(f).)

This bill:

1) Defines the following terms:
    a) "Covered entity" means a program or activity that requires a parent signature or consent form authorization, or an event in which a parent designates authority for an organization to act in loco parentis, that is offered primarily to youth outside of school hours, including periods when school is not in session, and that is not operated by a public or private elementary or secondary school, that may include programs related to expanded learning, visual or performing arts, athletics, recreation, or educational enrichment; "covered entity" does not include a business that is hosting or participating in a covered entity's program or activity for a field trip or other occasional activity, including amusement or water parks, zoos, aquariums, restaurants, state or county fairs, and movie theaters.
    b) "Covered information" means a picture, video, audio recording, likeness, attributed statement, personal information as defined under the CCPA, or any other identifying information.
    c) "Expanded learning" has the same meaning as in the Education Code, as specified.
    d) "Marketing purposes" means promotions, newsletters, brochures, social media, or other public-facing materials that describe the programs or solicit participation.
    e) "Public or private elementary or secondary school" means either of the following:
        i. An elementary or secondary school operated by the governing board of a school district or county office of education, or the governing body of a charter school.
        ii. An elementary or secondary school that has filed an affidavit with the Superintendent of Public Instruction and that reports a total enrollment of six or more students.

2) Prohibits a covered entity from using a youth's covered information for communications, marketing, educational, or training purpose unless the covered entity obtains the express written or electronic signature of the parent or guardian of the youth on a notice that complies with all of the following:
    a) The notice communicates the requested uses of the youth's covered information clearly but meaningfully, including a detailed list that includes all websites, brochures, or other materials or media where the covered entity is requesting to use the youth's covered information.

   b) The notice is contained in a single document or single website that is separate from enrollment forms, waivers of liability, and any other document.
   c) The notice includes, in clear and understandable language, that the parent or guardian is providing consent for use of the youth's covered information for communications, marketing, educational, or training purposes and includes a detailed list of all types of communications, marketing, educational, or training purposes for which consent is sought.
   d) The notice includes, in clear and understandable language, that the parent or guardian may revoke consent at any time and provides an e-mail address for submitting revocation.

3) Prohibits a covered entity from making enrollment or participation contingent upon a parent or guardian providing consent pursuant to 2), and requires the notice to clearly and conspicuously state that enrollment or participation is not contingent upon consent.

4) Prohibits a covered entity from selling covered information of a youth for any reason, regardless of whether the parent or guardian provided consent to that use pursuant to 2).

5) Permits a parent or guardian to revoke consent at any time during the youth's enrollment in the covered program and up to one year after the youth is no longer in the program.

6) Requires a covered entity to remove the youth's covered information from communications, marketing, educational, and training materials within seven days of receiving a notice of consent revocation under 5); the covered entity is not, however, required to remove covered information from communications, marketing, educational, or training materials that were printed prior to receiving a notice revoking consent.

7) Permits a parent or guardian to bring a civil action in a court of competent jurisdiction against a covered entity for a violation of the section created by this measure; a parent who prevails in an action may be awarded any of the following relief:
   a) Up to $2,500 for the first offense and $5,000 for any subsequent offenses, or a lesser amount as determined by the court, per youth who had their covered information disclosed.
   b) Injunctive or declaratory relief.
   c) Reasonable attorney's fees and costs.
   d) Any other relief the court deems appropriate.

8) Provides that the measure does not impair or impede any other rights, causes of action, claims, or defenses available under any other law, including, but not limited

to, the statutory right of publicity; and that the remedies are cumulative with any other remedies available under any other law.

COMMENTS

1. Author's comment

According to the author:

> Youth programs play an important role in supporting children and families, and parents should be able to trust that a minor's participation does not come at the cost of their privacy. Families participate in programs expecting a safe and supportive environment, not anticipating that images of their children could later be used in public-facing content without their knowledge or consent. AB 2007 requires youth-serving organizations to obtain written or electronic consent from a parent or guardian before using photos, videos, and other identifying information of minors for marketing purposes. AB 2007 further prohibits youth programs from making enrollment or participation contingent upon consent. By ensuring parents and guardians have the opportunity to review and approve how their child's information is used, AB 2007 establishes a simple and commonsense safeguard that protects a child's privacy while maintaining transparency and trust between youth organizations and the families they serve.

2. The incredibly depressing risks of posting photos of children on the internet

Back when social media was a new thing, the ability to easily share photos among friends and family seemed like all upside. For a while, it was not unusual for parents[1] to flood their social media channels with baby and kid photos. It soon became clear, however, that "sharenting" can have unintended consequences:

> Images of children posted online can be downloaded and used by others. One example of the misuse of photographs is called "digital kidnapping" where an image posted by a parent is used by another adult, and the child pictured is portrayed as belonging to the other adult. Another danger is that photos of children posted on social media can be shared to child pornography sites *and* the images can be traced back to the original Facebook page. In these cases, further information about the child can be gained, including the child's home address or school name. Additionally, sites now exist purely for the purpose of ridiculing images that have been posted on social media.[2]

---

[1] This analysis uses "parent" to include a legal guardian.
[2] Masur, *Sharenting: Should You Share Photos and Information About Your Kids Online?* (Aug. 29, 2024) Psychology Today, https://www.psychologytoday.com/us/blog/parenting-

The rise of generative AI, which can create photorealistic images of humans, increases the downsides. "Children's faces and likenesses are sensitive biometric data that can be scraped from social media posts and used to create deepfakes—AI-generated synthetic media that mimic real images, audio, or video."[3] A 2018 study suggested that photos posted online by parents "will account for two-thirds of identity fraud facing young people by the end of the next decade."[4] A New York Times investigation found that "an unprecedentedly huge facial recognition database called MegaFace" created a database of the likenesses of nearly 700,000 individuals using images scraped from photo storage sites like Flickr.[5]

Evidence suggests that many parents are unaware of the risks posed by sharing their kids' photos and videos online, but for those with that awareness, there's an increasing trend of keeping their kids' images off of social media.[6] For those parents who are working to protect their kids' digital footprint, however, their efforts can be undermined when their kids' schools and extracurricular programs fail to practice the same caution. For example:

> [A]n unnamed UK secondary school had recently been subjected to a blackmail attempt after criminals used the institution's website or social media accounts to take photos of schoolchildren and then, using AI tools, turned them into child sexual abuse material (CSAM). The blackmailers sent the images to the school and threatened to publish them online if they did not receive money.[7]

According to the author, there has been a problem of extracurricular programs and after-school activities declining to respect parents' wishes to keep their kids' faces off of the internet. The author reports that, although these programs do, in a formalistic sense, get parental consent before sharing, as a practical matter, parents have no way to decline. Tactics to compel consent include using an online consent form that doesn't give parents the option to decline specific terms; failing to provide contact information to a person at the program to withdraw consent; and, in at least one case, prohibiting a

---

matters/202408/sharenting-should-you-share-photos-and-information-about-your-kids. All links in this analysis are current as of June 19, 2026.

[3] Andoh, *What you need to know before sharing your child's life online* (Jun, 1, 2026) American Psychological Association, https://www.apa.org/monitor/2026/06/parents-children-sharing-online.

[4] Coughlan, *'Sharenting' puts young people at risk of online fraud* (May 20, 2018) BBC, https://www.bbc.com/news/education-44153754.

[5] Hill & Krolik, *How Photos of Your Kids Are Powering Surveillance Technology* (as corrected Oct. 29, 2019) New York Times, https://www.nytimes.com/interactive/2019/10/11/technology/flickr-facial-recognition.html.

[6] E.g., Conti, et al., *Sharenting: characteristics of parents publishing sensitive content of their children on online platforms* (Jul. 30, 2024) Italian Journal of Pediatrics, *available at* https://pmc.ncbi.nlm.nih.gov/articles/PMC11290302/.

[7] Milmo, *UK schools should remove pupils' online photos as AI blackmail threat grows, say experts* (May 7, 2026) The Guardian, https://www.theguardian.com/technology/2026/may/08/uk-schools-remove-pupils-photos-online-ai-blackmail-threat-grows.

child from participating in a program after the parent reached out to decline consent. This consent-or-nothing approach also leaves children who are facing more immediate threats from being displayed in public-facing content—such as a child whose parent has been restrained pursuant to a domestic violence restraining order—without recourse. Additionally, as the Assembly Judiciary Committee's analysis of this bill noted, certain jurisdictions prohibit photos of foster children from being published; making enrollment contingent upon consent to permitting the use of images will, necessarily, exclude those children entirely.

3. This bill prohibits after-school and extracurricular programs for minors from using minors' personal information, as defined, without parental consent

To ensure that parents don't have to choose between their kids' digital security and allowing their kids to participate in normal childhood activities, this bill establishes safeguards for youth-focused programs' use of a minor's image, likeness, or other personal information in their public-facing marketing materials. A program qualifies as a "covered entity" subject to the bill's requirements if it meets specified criteria, including that it requires written consent from a parent or guardian to participate and is directed primarily at youth. The bill expressly exempts, from the definition of "covered entity," a business that is hosting or participating in a covered entity's program or activity for a field trip or other occasional activity, such as a zoo, aquarium, or amusement or water park. The author has agreed to amendments to clarify these provisions.

The bill expressly prohibits a covered entity from making enrollment or participation contingent upon the provision of consent to the use of a youth's covered information. "Covered information" includes photos, video, and audio recordings featuring the child, as well as the child's likeness, statements attributed to the child, and the child's personal information protected under the CCPA. To use a child's covered information in communications, marketing, educational, or training materials, the covered entity must obtain consent through a notice that meets specified requirements. Furthermore, irrespective of parental consent, a covered entity cannot sell a youth's covered information for any reason. The author has agreed to amendments to streamline the notice requirements, including removing references to "electronic signatures"; under existing law, a "writing" in an agreement includes electronic signatures,[8] so the added reference is unnecessary.

With respect to the right to revoke consent, the bill permits a parent to revoke consent up to one year after the child is no longer enrolled in the program, to a period of one year post-enrollment. The bill also makes the revocation partially retroactive: when a parent revokes consent, the covered entity has seven days to remove the child's covered information from any digital materials featuring the child, but not from any printed materials that were printed prior to the revocation. The author has agreed to remove

[8] *See* Civ. Code, div. 3, pt. 2, tit. 2.5, §§ 1633.1 et seq.

the provision requiring the removal of pre-revocation materials; these amendments and others are set forth in Comment 4, below.

The bill authorizes a parent to bring a civil action against a covered entity that violates this bill's requirements. A prevailing parent may be awarded any or all of the following:

- Up to $2,500 for the first offense and up to $5,000 for any subsequent offenses, or a lesser amount as determined by the court, per youth who had their covered information disclosed.
- Injunctive or declaratory relief.
- Reasonable attorney's fees and costs.
- Any other relief the court deems appropriate.

The bill also specifies that this right of action, and the available remedies, are in addition to other existing rights, including California's right of publicity.

4. Stakeholder concerns and amendments

As noted above, the author recently amended the bill in response to concerns from extracurricular programs about the scope and feasibility of the bill's requirements. Municipal organizations, however, still have concerns about the bill. For example, the League of California Cities and the California Parks & Recreation Society noted all of the following:

- "The measure could…impact routine operational practices such as youth sports team recognition, tournament brackets, swim lesson certifications, scholarship fundraising materials, volunteer recognition, camp recap videos, and community event communications that families have long associated with local recreation programming. This goes well beyond existing privacy law protections and would impose substantial administrative burdens on agencies that operate with lean staffing."
- "The bill requires express written consent obtained through a standalone notice document that must be entirely separate from enrollment forms, liability waivers, and any other materials. For public agencies that process thousands of registrations per season — often through online registration systems — this requirement would necessitate a complete overhaul of registration workflows and technology infrastructure. Unlike private businesses, public agencies cannot easily pass these compliance costs on to consumers."
- "The bill would authorize civil actions with damages of up to $5,000 per youth whose covered information is disclosed, plus injunctive relief, attorney's fees, and other remedies. For public agencies operating community recreation programs on tight budgets, even inadvertent technical violations — such as including a child's photo in a newsletter before a new consent form is completed — could result in significant financial exposure. This creates a chilling effect on ordinary, community-facing communications that serve the public interest."

- "The bill's revocation provision, as currently drafted, creates ambiguity for local agencies. While it seeks to give parents the ability to revoke consent for the use of their child's information, the requirement to remove the electronic form of that information does not account for local agencies' obligations around public records and records retention. Without clarification, the bill could be interpreted to require the deletion or alteration of records that agencies are required to preserve."

In response to these concerns and others, the author has agreed to a number of amendments, which will be taken in the Senate Privacy, Digital Technologies, and Consumer Protection. The amendments are set forth below, subject to any nonsubstantive changes the Office of Legislative Counsel may make.

Amendment 1

At page 2, in lines 9-15, and page 3, lines 1-2, delete the existing definition of "covered entity" and insert:

(1) (A) "Covered entity" means an entity or organization that operates a covered program.

Amendment 2

At page 3, in line 4, after "entity's" insert "covered"

Amendment 3

At page 3, between lines 7 and 8, insert:

(C) "Covered program" means a program or activity that is all of the following:

(I) Requires a parent signature, consent form authorization, or an event in which a parent provides written authorization for an organization to act in loco parentis,

(II) Offered primarily to youth outside of school hours, including periods when school is not in session, and that is not operated by a public or private elementary or secondary school.

(D) Examples of a covered program include, but are not limited to, programs related to expanded learning, visual or performing arts, athletics, recreation, or educational enrichment, and day and overnight camps.

Amendment 4

At page 3, in line 14, add "(A)" after "(4)", and between lines 16 and 17, insert:

(B) "Marketing purposes" does not include materials shared with parents or guardians of the youths participating in the program, provided that the materials cannot be accessed by the general public.

Amendment 5

At page 3, between lines 24 and 25, insert:

(b) A covered entity shall not make a youth's enrollment or participation in a covered program contingent upon a parent or guardian consenting to the covered program's use of the youth's covered information for any communications, marketing, educational, or training purpose.

Amendment 6

At page 3, in lines 31-32, delete "express written or electronic signature of the parent or guardian of the youth" and insert "youth's parent or guardian's express written consent"

Amendment 7

At page 3, in lines 34-38, modify subparagraph (A) to read:

(A)The notice communicates the requested uses of the youth's covered information clearly and meaningfully, including a description of all of the proposed uses of the youth's covered information, a description of the types of materials or media in which the information may be used, and a list of websites on which the covered information may be published.

Amendment 8

At page 4, in lines 1-2, delete "single internet website" and insert "separate page within an online form"

Amendment 9

At page 4, delete "and" in line 8 and delete all of lines 9-11, and insert "as set forth in the description required pursuant to subparagraph (A)."

Amendment 10

At page 4, in line 14, delete "and" and delete all of lines 15-16.

Amendment 11

At page 4, in lines 22-27, delete the existing paragraph (2) and insert:

(E) The notice clearly and conspicuously states that the youth's enrollment or participation is not contingent upon consent.

(F) The notice provides an electronic mail address at which the parent or guardian can contact the program relating to the scope of consent, revocation of consent, or other issues relating to a youth's covered materials.

Amendment 12

At page 4, delete lines 36-39 and insert:

(B) A revocation pursuant to subdivision (B) must be made through the electronic mail address provided pursuant to subparagraph (F) of paragraph (1) of subdivision (b).

Amendment 13

At page 5, in line 3, insert "published or" in between "were" and "printed"

6. Arguments in support

According to the California Catholic Conference:

The California Catholic Conference particularly appreciates that the bill requires express written parental consent after providing clear notice regarding how a youth's identifying information will be used. Equally important, the bill prohibits organizations from conditioning a child's participation in a program on the provision of such consent. This protection ensures that families are not forced to choose between participation opportunities and their child's privacy rights.

AB 2007 also appropriately prohibits the sale or sharing of a youth's identifying information and limits the use of that information solely to the purpose for which consent was granted. These provisions provide meaningful safeguards at a time when concerns regarding privacy, data collection, digital marketing, and the use of children's personal information continue to grow.

Catholic Social Teaching emphasizes the inherent dignity of every human person and the responsibility of society to protect vulnerable populations, especially children. The principles of human dignity, subsidiarity, and the common good all support policies that empower families, respect parental authority, and protect children from exploitation or misuse of their personal information. AB 2007 advances these principles by placing decision-making authority where it belongs—with parents and guardians—while establishing clear and reasonable expectations for organizations serving youth.

SUPPORT

California Catholic Conference

OPPOSITION

None received.

RELATED LEGISLATION

Pending legislation: SB 1247 (Padilla, 2026) authorizes a child influencer, as defined, to demand the removal of family vlogging content featuring them when they were a minor. SB 1247 is pending before the Assembly Judiciary Committee.

Prior legislation: None known.

PRIOR VOTES:

Assembly Floor (Ayes 72, Noes 0)
Assembly Appropriations Committee (Ayes 15, Noes 0)
Assembly Judiciary Committee (Ayes 12, Noes 0)
Assembly Privacy and Consumer Protection Committee (Ayes 15, Noes 0)

****