

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

AB 1946 (Wicks)
Version: May 21, 2026
Hearing Date: June 30, 2026
Fiscal: Yes
Urgency: No
AWM

SUBJECT

Reporting mechanism: child sexual abuse material

DIGEST

This bill modifies the provisions relating to a social media platform's obligation to provide a mechanism to report child sexual abuse material (CSAM) on the platform, including to harmonize certain requirements with federal law, and modifies the conditions under which a social media platform can be held liable for facilitating or aiding and abetting commercial sexual exploitation.

EXECUTIVE SUMMARY

Social media platforms are rife with CSAM; platforms are not only used to exchange CSAM, but also to facilitate the creation of CSAM. Once a CSAM file is uploaded or posted online, it can be circulated for years, leaving survivors to relive and experience this abuse long after it originally occurred. Although social media companies claim they take the problem of CSAM seriously, the problem persists.

In 2023, the Legislature enacted AB 1394 (Wicks, Ch. 579, Stats. 2023), establishing a first-in-the-nation framework for survivors to report CSAM on social media platforms for its removal. AB 1394 went into effect in 2025. Since then, stakeholders have found that there are gaps in the accessibility, effectiveness, and accountability measures put in place by AB 1394.

This bill is intended to correct those issues by updating and strengthening the mechanism by more clearly outlining accessibility standards, expanding access to the reporting mechanism to all users, and aligning existing law's definitions and timeline with the recently passed federal TAKE IT DOWN Act. This bill also permits public prosecutors to file civil actions against platforms who are violating the reporting mechanism requirements, and expands an existing cause of action available when a social media platform knowingly facilitates, or aids and abets, commercial sexual

exploitation of a minor or nonminor dependent. The author has agreed to minor amendments to clarify the cause of action available to a nonreporting user depicted in CSAM and to ensure that audits provided to the Attorney General do not become public records.

This bill is sponsored by the Children's Advocacy Institute at the San Diego University School of Law and is supported by 3Strands, the California Family Council, the California Coalition for Children's Safety and Health, the California District Attorneys Association, the California Institute for Technology & Democracy, Common Sense Media, Jewish Family and Children's Services, and the Organization for Social Media Safety. The Committee has not received timely opposition to this bill, but tech industry trade groups have expressed concerns. The Senate Privacy, Digital Technologies, and Consumer Protection Committee is set to hear this bill on the day before this Committee's hearing.

PROPOSED CHANGES TO THE LAW

Existing constitutional law:

- 1) Provides that the U.S. Constitution, and the Laws of the United States, are the supreme law of the land. (U.S. Const., art. VI, cl. 2.)
- 2) Provides that Congress shall make no law abridging the freedom of speech. (U.S. Const., 1st amend. (the First Amendment) & 14th amends.; 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).)
- 3) 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:

- 1) Defines "child pornography" as any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, as defined, which satisfies one of the following:
 - a) The production of such visual depiction involves the use of a minor engaging in sexually explicit conduct.
 - b) Such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct.

- c) Such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct. (18 U.S.C. § 2256(8).)
- 2) Provides that no provider or user of a website shall be treated as the publisher or speaker of any information provided by another information content provider, and that no provider of a website shall be held liable on account of any action voluntarily taken in good faith to restrict the availability of materials that the provider determines to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected. (47 U.S.C. § 230(c) (Section 230).)
- 3) Provides that no cause of action may be brought and no liability may be imposed under any state or local law that is inconsistent with Section 230. (47 U.S.C. § 230(e).)
- 4) Establishes the Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks (TAKE IT DOWN) Act, which defines the following relevant terms:
 - a) “Consent” means an affirmative, conscious, and voluntary authorization made by an individual free from force, fraud, duress, misrepresentation, or coercion.
 - b) “Digital forgery” means any intimate digital depiction of an identifiable individual created through the use of software, machine learning, artificial intelligence, or any other computer-generated or technological means, or altering an authentic visual depiction, that, when viewed as a whole by a reasonable person, is indistinguishable from an authentic visual depiction of the individual.
 - c) “Identifiable individual” means an individual who appears in whole or in part in an intimate visual depiction, and whose face, likeness, or other distinguishing characteristic (including a unique birthmark or other recognizable feature) is displayed in connection with such intimate visual depiction.
 - d) “Intimate visual depiction” means a visual depiction that depicts the uncovered genitals, pubic area, anus, or post-pubescent female nipple of an identifiable individual, or the display or transfer of bodily sexual fluids onto or from the body of an individual, as specified, or engaging in sexually explicit conduct.¹ (47 U.S.C. § 223(h)(1).)

¹ The federal definition of “intimate visual depiction” includes a drafting error which caused the “engaged in sexually explicit conduct” prong to be nestled within the “display or transfer of bodily fluids” prong. (See 15 U.S.C. § 6851(a)(5)(A).) Federal legislation that would correct this error is pending before Congress. (See HR 8516 (119th Cong., 2d Sess), § 501.) The same legislation would expand the federal civil action for nonconsensual sexual imagery to include digitally created sexual imagery, including imagery generated by AI. (*Ibid.*)

- 5) Makes it a crime for any person, in interstate or foreign commerce, to use an interactive computer service to knowingly publish an intimate visual depiction of an identifiable individual, including a digital forgery, as follows:
 - a) If the person is not a minor, when the intimate visual depiction was obtained or created under circumstances in which the person knew or reasonably should have known that the identifiable individual had a reasonable expectation of privacy, the content depicted was not voluntarily exposed by the individual, the content depicted is not a matter of public concern, and the publication of the intimate visual depiction is intended to cause harm to the identifiable individual.
 - b) If the person is a minor, when the depiction is posted with the intent to abuse, humiliate, harass, or degrade the minor, or to arouse or gratify the sexual desire of any person. (47 U.S.C. § 223(h)(2) & (3).)
- 6) Requires a covered platform to establish a process whereby an identifiable individual, or an authorized person acting on their behalf, may notify the platform of an intimate visual depiction on the platform and request its removal, with information sufficient for the platform to identify the individual and to locate the intimate visual depiction in question.
 - a) The platform must provide a clear and conspicuous notice of the removal process that is easy to read, in plain language, and provides information regarding the platform's obligations, including how to submit a removal notice.
 - b) Upon receiving a valid removal request, a covered platform shall, as soon as possible, but not later than 48 hours after receiving the request, remove the intimate visual depiction and make reasonable efforts to identify and remove any known identical copies of such depiction.
 - c) A platform's failure to remove an intimate visual depiction after receiving a valid request is treated as a violation of specified federal laws and may be enforced by the Federal Trade Commission. (47 U.S.C. 223a.)

Existing state law:

- 1) Defines the following relevant terms:
 - a) "Child pornography," "identifiable minor," and "minor" have the same meaning as in federal law.
 - b) "Child sexual abuse material" means either of the following:
 - i. Child pornography.
 - ii. Obscene matter that depicts a minor personally engaging in, or personally simulating, sexual conduct.
 - c) "Identifiable minor" has the same meaning as in federal law.
 - d) "Obscene matter" means matter, taken as a whole, that to the average person, applying contemporary statewide standards, appeals to the prurient interest, that, taken as a whole, depicts or describes sexual conduct in a patently

offensive way, and that, taken as a whole, lacks serious literary, artistic, political, or scientific value.

- e) "Social media platform" means a public or semipublic internet-based service or application that has users in California and that meets specified criteria relating to connecting users for social interaction and the creation of a profile within the platform; "social media platform" does not include email-only services, cloud storage, a standalone direct messaging service that provides end-to-end encryption, or an internet service or application owned or operated by a tax-exempt nonprofit organization. (Civ., § 3273.65; *see also* Bus. & Prof. Code, § 22675; Pen. Code, § 311.)
- 2) Requires a social media platform to do all the following:
- a) Provide an accessible mechanism for California users to report material to the platform that the user reasonably believes is CSAM that is displayed, stored, or hosted on the platform.
 - b) Collect information reasonably sufficient to enable the platform to contact the reporting user and contact the user in writing by a method chosen by the user that is not in control of the social media company that operates the platform.
 - c) Permanently block the instance of reported material, and make reasonable efforts to remove and block other instances of the same material from being viewable on the platform, if there is a reasonable basis to believe it is CSAM; it is stored, displayed, or hosted on the platform; and the report contains basic identifying information sufficient to permit the platform to locate the reported material.
 - d) Provide a written confirmation regarding receipt of the report within 36 hours of the report, with a description of the schedule of regular written updates that the platform is required to make.
 - e) Provide a written update to the reporting user as to the status of the platform's handling of the reported material using the information collected from the reporting user, as described above.
 - f) Issue a final written determination to the reporting user stating whether the material has been determined to be CSAM displayed, stored, or hosted on the social media platform.
 - g) Comply with the requirements described above within 30 days, unless there are circumstances beyond the reasonable control of the platform, in which case compliance must be within 60 days; notice of the delay must be provided to the reporting user within 48 hours of the time the platform knew the delay was likely to occur. (Civ. Code, § 3273.66)
- 3) Provides that a social media platform that fails to comply with the requirements described in 2) shall be liable to the reporting user for the following:
- a) Actual damages sustained by the reporting user as a result of the violation.
 - b) Statutory damages of no more than \$250,000 per violation; if the platform permanently blocks the reported material prior to the commencement of the

- action, the maximum statutory damage amount is \$125,000; or, as set forth in 4), the maximum statutory damage amount is \$75,000 if specified conditions are met.
- c) Reasonable attorney's fees and costs.
 - d) Any other relief the court deems proper. (Civ. Code, § 3273.67(a).)
- 4) Provides that a social media platform's liability under 3) for a violation of 2) arising from the platform's failure to permanently block reported CSAM, or its failure to provide the reporting user with a compliant written confirmation, update, or final report, is a maximum of \$75,000 per violation if the social media platform meets all of the following requirements:
- a) The social media platform registers with, and participates in, the National Center for Missing and Exploited Children's Take It Down service or its successor.
 - b) The social media platform receives updated hash values for identified CSAM from the National Center for Missing and Exploited Children's Take It Down Service, or its successor, at least once every 36 hours.
 - c) Within 36 hours of receiving updated hash values, the social media platform removes CSAM identified by the hash values from the platform.
 - d) The social media platform reports identified CSAM to the National Center for Missing and Exploited Children's CyberTipline, as required by federal law.
 - e) The social media platform provides to a reporting user specified information when a user reports CSAM to the platform directly. (Civ. Code, § 3273.67(a)(2).)
- 5) Requires the court, in determining the amount of statutory damages available pursuant to 3) or 4), to consider the willfulness and severity of the violation and whether the social media platform has previously violated 2). (Civ. Code, § 3273(a)(2)(B).)
- 6) Provides that, where a social media platform that fails to comply with its removal, confirmation, update, and final report obligations within 60 days after the date on which material was first reported, there is a rebuttable presumption that the social media platform is liable for statutory damages. (Civ. Code, § 3273(b).)
- 7) Establishes factors that a court must consider when determining the amount of damages, fine, or civil penalty in an civil action brought by, or on behalf of, a minor or nonminor dependent against a person who engaged in any act of sexual exploitation of a minor or nonminor dependent, and authorizes the court to award treble the statutorily authorized amount if certain factors are met. (Civ. Code, § 3345.1(b).)
- 8) Prohibits a social media platform from knowingly facilitating, aiding, or abetting commercial sexual exploitation. (Civ. Code, § 3345.1(g).)

- 9) Provides that, in an action for a violation of 8), a court shall award statutory damages of not more than \$4 million and not less than \$1 million for each act of commercial sexual exploitation facilitated, aided, or abetted by the social media platform. (Civ. Code, § 3345.1(g)(2).)
- 10) Provides that a social media platform shall not be deemed to be in violation of 8) if it demonstrates all of the following:
 - a) The social media platform instituted and maintained a program of at least biannual audits of its designs, algorithms, practices, affordances, and features to detect designs, algorithms, practices, affordances, or features that have the potential to cause or contribute to violations of 8).
 - b) The social media platform took action, within 30 days of the completion of the audit, to mitigate or eliminate the reasonably foreseeable risk that a design, algorithm, practice, affordance, or feature violates, or contributes to, a violation of 8).
 - c) The social media platform provided copies of the audit to its board members, and a description of any corrective actions taken, within 90 days of the audit's completion. (Civ. Code, § 3345.1(g)(3).)
- 11) Provides that a social media company is deemed to have knowledge of commercial sexual exploitation under 8) if all of the following are true:
 - a) Material was reported to a social media platform using the reporting mechanism required in 2) for four consecutive months.
 - b) The material is CSAM depicting the reporting individual and displayed, stored, or hosted on the platform.
 - c) The reported material was first displayed, stored, or hosted on the platform on or after January 1, 2025. (Civ. Code, § 3345.1(g)(4).)
- 12) Defines, for purposes of 8)-11), the following terms:
 - a) "Commercial sexual exploitation" means an act committed for the purpose of obtaining property, money, or anything else of value in exchange for, or as a result of, a sexual act of a minor or nonminor dependent, including acts that constitute a violation of specified Penal Code provisions.
 - b) "Facilitate, aid, or abet" means to deploy a system, design, feature, or affordance that is a substantial factor in causing minor users to be victims of commercial sexual exploitation. (Civ. Code, § 3345.1.)

This bill:

- 1) Modifies the provisions enacted through AB 1394 (Wicks, Ch. 579, Stats. 2023), as set forth below.
- 2) Adds or modifies the following definitions:

- a) "Block" means to remove from being publicly viewable on the social media platform.
 - b) "Obscene matter" is amended to mean an intimate visual depiction involving an identifiable individual who is, or reasonably appears to be, a minor.
 - c) "Clear and conspicuous" is amended to have the same definition as in Business and Professions Code section 17601.
 - d) "Dark pattern" has the same meaning as defined in existing state law.
 - e) "Depicted individual" means a person who is depicted, including through the use of AI, as a minor in CSAM on a social media platform.
 - f) "Digital forgery" means an intimate visual depiction of an identifiable individual created through the use of software, machine learning, artificial intelligence, or any other computer-generated or technological means, including by adapting, modifying, manipulating, or altering an authentic visual depiction that, when viewed as a whole by a reasonable person, is indistinguishable from an authentic visual depiction of the individual.
 - g) "Hash" means a unique, fixed-length alphanumeric value generated from the contents of an image.
 - h) "Hash-matching process" means a process by which images and videos of CSAM can be converted into hashes and used to identify known child sexual abuse material.
 - i) "Identifiable individual" means an individual that meets both of the following criteria:
 - i. The individual appears in whole or in part in an intimate visual depiction.
 - ii. The individual's face, likeness, or other distinguishing characteristic, including a unique birthmark or other recognizable feature, is displayed in connection with that intimate visual depiction.
 - j) "Intimate visual depiction" means a visual depiction that depicts, whether through a digital forgery or otherwise, any of the following:
 - i. The uncovered genitals, pubic area, anus, or postpubescent female nipple of an identifiable individual.
 - ii. The display or transfer of bodily sexual fluids onto any part of the body of an identifiable individual or from the body of an identifiable individual.
 - iii. An identifiable individual engaging in sexually explicit conduct.
 - k) "Sexually explicit conduct" has the same meaning as in specified federal law.
- 3) Modifies the AB 1394 reporting mechanism, as follows:
- a) Requires the mechanism to be clear and conspicuous, and prohibits the mechanism from using dark patterns.
 - b) Requires the mechanism to accept reports of material sent or received through direct messaging systems.
 - c) Eliminates the requirement that the reporting user be an identifiable minor depicted in the material.

- 4) Requires a social media platform to do all of the following in connection with a report made through the AB 1394 reporting mechanism:
 - a) Ensure that any report submitted is reviewed through a hash-matching process.
 - b) Ensure that the report is reviewed by a natural person if both of the following are true:
 - i. There is not an established or known hash match to CSAM with respect to the reported material.
 - ii. The material is not otherwise blocked.
- 5) Prohibits a social media platform from using dark patterns to influence a reporting user's choice of contact method for purposes of the social media platform's obligation to contact the user.
- 6) Shortens the timeframes for the social media platform's contact, blocking, and written update requirements under AB 1394, as follows:
 - a) The default time for compliance is shortened from 30 days to 48 hours.
 - b) The timeframe for compliance if the social media platform cannot comply within 48 hours, due to circumstances beyond the reasonable control of the social media platform, is shortened from 60 days to 5 days.
- 7) Requires a social media platform to restore availability or functionality of the AB 1394 reporting mechanism if it is unavailable or nonfunctional.
- 8) Authorizes the Attorney General, a district attorney, a city attorney, or county counsel to bring an action against a social media platform that is in violation of AB 1394 and to recover a civil penalty of up to \$250,000 for each day that the reporting mechanism is in violation of AB 1394, plus reasonable attorney's fees and costs.
 - a) A social media company shall not be liable if the reporting mechanism is in violation of AB 1394 for any period for which the company demonstrates, by clear and convincing evidence, that the violation was caused by circumstances beyond the company's reasonable control and not due to any act or omission by the company, including a failure to implement or maintain adequate systems, processes, or safeguards.
 - b) The penalties shall continue to accrue daily until the social media company restores full functionality of the reporting mechanism, as required by law.
 - c) In addition to monetary penalties, the Attorney General, a district attorney, a city attorney, or county counsel may seek injunctive relief to compel a social media company to immediately restore and maintain a fully functional reporting mechanism in compliance with AB 1394; the court may issue temporary, preliminary, or permanent injunctive relief as necessary to prevent ongoing violations.

- 9) Exempts, from the private right of action for a reporting user who is a depicted individual available under AB 1394, causes of action arising from a violation of the requirement to provide a reporting mechanism, as specified.
- 10) Provides that a depicted individual who is not a reporting user may bring a civil action for a violation of AB 1394 under the same terms as a depicted individual who is a reporting user.
- 11) Provides that any penalty collected by the Attorney General in an action for a violation of AB 1394, less reasonable attorney's fees and costs, shall be posted into the Survivor Support Fund established under state law.
- 12) Adds, to the list of factors a social platform must demonstrate to avoid liability for knowingly facilitating, aiding, or abetting commercial sex exploitation, that the social media platform submitted biannual audits to the Attorney General and, if requested, to a district attorney, city attorney, or county counsel.
- 13) Modifies the circumstances in which a social media platform is deemed to have knowledge of sexual exploitation on the platform when material has been reported to a social media platform through the AB 1394 platform, from requiring the material be reported for four consecutive months to requiring only that the material have been reported.
- 14) Adds a severability clause.

COMMENTS

1. Author's comment

According to the author:

Although AB 1394 created a framework and mechanism to combat the proliferation of CSAM, there are gaps within the existing law that still allow CSAM to spread on social media platforms. AB 1946 would fill in some of these gaps and expand the mechanism so that the process to report CSAM and the law is clear and functional.

2. CSAM on social media

As explained in the Senate Privacy, Digital Technologies, and Consumer Protection Committee's analysis of this bill:

CSAM refers to any visual depiction of sexually explicit conduct involving a person under the age of 18. As outlined by the United States Department of Justice, CSAM is one of the most heinous crimes:

Underlying every sexually explicit image or video of a child is abuse, rape, molestation and/or exploitation. The production of CSAM creates a permanent record of the child's victimization.²

The National Center for Missing & Exploited Children (NCMEC) further explains the horrifying nature of CSAM:

Not only do these images and videos document victims' exploitation and abuse, but when these files are shared across the internet, child victims suffer re-victimization each time the image of their sexual abuse is viewed. In a recent survey led by the Canadian Centre for Child Protection, 67% of CSAM survivors said the distribution of their images impacts them differently than the hands-on abuse they suffered because the distribution never ends and the images are permanent.

It's important to remember CSAM consists of much more than just images and video files. While CSAM is seen and transmitted on computers and through other technology, these images and videos depict actual crimes being committed against children. The human element, children at risk, must always be considered when talking about this offense that is based in a high-tech world.

The disturbing reality is that the internet platforms we use every day to connect with each other and share information, including social media, online gaming, and e-mail, are now being used to disseminate and collect CSAM. CSAM can be found in virtually any online realm.³...

Concerningly, social media has emerged as a popular vector for CSAM. As noted in NCMEC's 2025 CyberTipline Reports by Electronic Services Providers, Snapchat, TikTok, X, WhatsApp, Instagram, and Facebook each recorded over 500,000 reports of CSAM.⁴ Furthermore, a research report by Protect Children revealed that 29 percent of individuals searching for CSAM on dark web search engines found CSAM on a social media platform.⁵ Exacerbating this is the fact that social media is not only a popular place to trade CSAM but also to arguably create it. A Forbes review of TikTok livestreams noted that viewers frequently commented on young girls' livestreams to create explicit content. The article provides:

² *Child Sexual Abuse Material* (2021) Department of Justice, <https://www.justice.gov/d9/2023-06/child-sexual-abuse-material-2.pdf>. All internet citations are current as of June 7, 2026.

³ *Child Sexual Abuse Material Overview* (2018) National Center for Missing & Exploited Children, <https://ncmec.org/theissues/csam>.

⁴ *2025 CyberTipline Reports by Electronic Service Providers* (2026) National Center for Missing & Exploited Children, <https://www.missingkids.org/content/dam/missingkids/pdfs/2025-reports-by-esp.pdf>.

⁵ *Tech Platforms Used by Online Child Sexual Abuse Offenders* (2024) Protect Children ry, https://bd9606b6-40f8-4128-b03a-9282bdcfff0f.usrfiles.com/ugd/bd9606_0d8ae7365a8f4bfc977d8e7aeb2a1e1a.pdf.

The transactions are happening in a public online forum open to viewers almost anywhere on the planet. Some of the demands are explicit – like asking girls to kiss each other, spread their legs or flash the camera – and some harder to detect, masked with euphemisms. Commenters say ‘outfit check’ to get a complete look at a girl’s body; ‘pedicure check’ to see their feet; ‘there’s a spider on your wall’ to get girls to turn around and show their rears; and ‘play rock-paper-scissors to encourage girls to flirt-fight or wrestle with each other. Phrases like ‘put your arms up’ or ‘touch the ceiling’ are often directed at girls in crop tops so viewers can see their breasts and stomachs. And many simply coax girls to show their tongues and belly buttons or do handstands and splits. In return, the girls are showered with virtual gifts, like flowers, hearts, ice cream cones and lollipops, that can be converted to cash.⁶

AI further complicates CSAM’s spread. When used responsibly, AI can be leveraged to combat the dissemination of CSAM. Advances such as machine learning classifiers provide novel ways for platforms and websites to detect and remove CSAM; this is certainly a welcome and important tool. However, the widespread adoption of generative AI (GenAI) has led to a dramatic increase in deepfake CSAM. NCMEC’s 2024 CyberTipline Report noted a 1,325 percent increase in GenAI related CSAM reports from 2023 to 2024. This corresponded to 4,700 reports in 2023 and 67,000 reports in 2024. In 2025, NCMEC received 1.5 million reports with a GenAI nexus.⁷ More than 1.1 million of these reports related to CSAM detection in AI training datasets.

3. This bill refines existing laws relating to social media companies’ obligations to prevent the display of CSAM on their platforms

In 2023, the Legislature enacted AB 1394 (Wicks, Ch. 579, Stats. 2023), which required a social media company to maintain a CSAM reporting mechanism on its platform and to respond to reports within specified timeframes.⁸ Under AB 1394, a platform can be liable for damages if it fails to take action to remove reported CSAM; AB 1394 also created a heightened available remedy when a social media platform knowingly facilitates, or aids and abets, the commercial exploitation of a minor or nonminor dependent conducted through the platform.⁹ AB 1394 became operative in 2025.

⁶ Alexandra Levine, *How TikTok Live Became ‘A Strip Club Filled with 15-Year-Olds’* (April 27, 2022), Forbes, <https://www.forbes.com/sites/alexandralevine/2022/04/27/how-tiktok-live-became-a-strip-club-filled-with-15-year-olds/?sh=734b448162d7>.

⁷ 2025 *CyberTipline Report* (2026) National Center for Missing & Exploited Children, <https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata>.

⁸ Civ. Code, § 3273.66.

⁹ *Id.*, § 3345.1.

This bill is intended to fix issues that have arisen since AB 1394's implementation. Much of the bill streamlines and strengthens AB 1394's reporting mechanism requirements, including by:

- Permitting persons other than the minor featured in the CSAM to report CSAM through the reporting mechanism.
- Requiring the social media platform to contact a reporting user through the contact method chosen by the user.
- Shortening the timeframe in which the social media platform must review and respond to a report, to 48 hours, or, if the platform cannot respond due to circumstances beyond its control, within five days.

The bill also harmonizes certain definitions and requirements with the federal TAKE IT DOWN Act, which was enacted after the passage of AB 1394, and modifies AB 1394's remedies.

The Senate Privacy, Digital Technologies, and Consumer Protection Committee considered this bill from an overall policy standpoint and passed it with a vote of x-y. This analysis examines, in the comments below, the bill's civil penalty provisions and the constitutional issues underpinning the bill.

4. The civil remedies added or modified by this bill

As noted above, this bill expands the remedies established in AB 1394 in a few ways.

First, the bill permits a depicted individual who is not a reporting user to bring an action for a violation of the CSAM reporting mechanism requirements. Given that the person depicted in the CSAM is person who suffers the most as a result of a platform's failure to timely remove a victim's images, this limited expansion of AB 1394's private right of action appears logical. The author has agreed to a minor amendment to clarify that, in the event that a depicted individual has reached the age of majority, they can pursue an action on their own behalf.

Second, the bill authorizes the Attorney General, a district attorney, a city attorney, or a county counsel to bring an enforcement action against a platform in violation of AB 1394, as amended by this bill. To ensure that a platform is not unfairly punished for violations caused by issues caused by other actors — e.g., an AWS outage that renders the platform's reporting infrastructure mechanism inoperable — the bill specifies that a social media company shall not be liable for a violation relating to the reporting mechanism for any period for which the social media company can demonstrate, by clear and convincing evidence, that the violation was caused by circumstances beyond the social media platform's reasonable control and not due to any act or omission by the company, as specified.

Third, the bill authorizes the Attorney General, a district attorney, a city attorney, or a county counsel to seek injunctive relief to compel a social media company to

immediately restore and maintain a fully functional reporting mechanism as required by law. Although not expressly characterized as such, the injunction authorized by this bill is a “mandatory injunction” because it would require a platform to take an immediate action.¹⁰ An injunction that “requires no action and merely preserves the status quo” is known as a “prohibitory injunction.”¹¹ Unless the Legislature otherwise specifies, a mandatory injunction will be stayed on appeal, while a prohibitory injunction will take effect immediately.¹²

Fourth, this bill modifies the conditions in which a victim of commercial sexual exploitation may bring a cause of action against a social media platform that knowingly facilitated, or aided and abetted, in their commercial sexual exploitation:

- The bill adds, to the list of conditions allowing a platform to avoid liability entirely, the requirement that a platform submit its biannual child exploitation prevention audits to the Attorney General or, upon request, a district attorney, city attorney, or county counsel. The social media platform is not required to do so – it’s simply an option if they want to take advantage of the liability safe harbor. The bill does not, however, provide any privacy protections for the audits, which may contain sensitive personal and/or company information. The author has, therefore, agreed to amend the bill to provide that these audit reports are not subject to the Public Records Act when provided to a public prosecutor.
- The bill reduces the timeframe before which a social media platform is deemed to have knowledge of commercial sexual exploitation based on a report of CSAM on the platform, from a period of four months during which the material was reported to the platform each month, to upon receipt of a report. Given the overwhelming evidence that social media platforms are already aware that their platforms are being used to exchange CSAM and traffic children, there does not appear to be a reason to give a platform four months’ worth of the benefit of the doubt.

5. Constitutional considerations

This Committee’s analysis of AB 1394 contained a thorough examination of the First Amendment and Section 230 questions raised by that bill. The author took amendments in response to concerns raised by the Committee analysis, and that amended language remained in the version of the bill that was ultimately enacted and signed.

As discussed throughout this analysis, this bill does not implement a wholly new program, but rather modifies the notification, takedown, and remedies provisions put in place by AB 1394. Moreover, in the years since AB 1394 took effect, it does not

¹⁰ *Daly v. San Bernardino County* (2021) 11 Cal.5th 1030, 1035.

¹¹ *Ibid.*

¹² *Ibid.*

appear that there have been any lawsuits challenging AB 1394. It is not, therefore, necessary to conduct an entirely new constitutional analysis.

Many of the bill's changes to AB 1394's notice-and-takedown structure align with the federal TAKE IT DOWN Act. For example, this bill shortens a platform's required time to respond to a removal request from 30 days to 48 hours; 48 hours is the removal timeframe under TAKE IT DOWN.¹³ Harmonizing AB 1394 with existing federal obligations should prevent, rather than invite, arguments that AB 1394 is preempted by federal law or that AB 1394's provisions violate the First Amendment.

Certain tech industry representatives have raised "concerns" that portions of the bill may implicate the First and Fourth Amendment; these concerns are listed in greater detail in Comment 7, below, and addressed here:

- Hash-matching concerns: this bill requires a platform, upon receipt of a report of CSAM, to review the reported material through a hash-matching process for known CSAM images or, if there is no established hash, require a human review to determine if the content is CSAM. To the extent a platform subsequently reports to law enforcement CSAM identified through these processes, it is possible that the Fourth Amendment could be implicated. The Fourth Amendment has a "private search" exception for searches conducted by private parties independent of law enforcement.¹⁴ Here, however, the bill imposes a state mandate to hash-match or visually inspect all reported material without a warrant.¹⁵ The Fourth Amendment is outside this Committee's jurisdiction, but the author may wish to continue working with stakeholders to ensure that these requirements will not have unintended consequences.
- CSAM definition: this bill expands the definition of CSAM to include a depiction of an identifiable individual who "is, or reasonably appears to be," a minor. The "reasonably appears to be" prong of this definition could be interpreted in a couple of ways. To the extent it applies to AI-generated or otherwise forged images that de-age an identified individual to create CSAM, it is hard to see how the First Amendment would protect such material. To the extent that this definition could be interpreted to extend to sexual material involving adults who appear to be minors, it is true that sexual content involving adults receives some First Amendment protection, while CSAM does

¹³ 47 U.S.C. § 223a(a)(3).

¹⁴ E.g., *United States v. Maher* (2d Cir. 2024) 120 F.4th 297, 311-312.

¹⁵ By comparison, the federal law that requires a provider of a website to report instances of online sexual exploitation of children to law enforcement as soon as possible expressly states that the provider is not required to "affirmatively search, screen, or scan" for such material. (18 U.S.C. § 2258A.) Providers are free to conduct such affirmative searches and scans as a matter of company policy (and many do), but when the material is turned over to law enforcement, the Fourth Amendment still prevents law enforcement from investigating the material beyond the scope of the provider's private search without a warrant. (*United States v. Wilson* (9th Cir. 2021) 13 F.4th 961, 971; see also *Maher*, *supra*, 120 F.4th at p. 318.)

not.¹⁶ Whether the state's compelling interest in protecting against the proliferation of CSAM justifies some chilling of sexual content involving individuals who could reasonably be mistaken for minors is ultimately a question for the courts, but given the unrelenting problem of CSAM on social media, the state has a strong case in the affirmative.

- Digital forgeries: this bill extends AB 1394 to "digital forgeries," i.e., material that has been AI-generated or otherwise altered to depict an intimate visual depiction of an identifiable individual. Federal law already prohibits the online publication of digital forgeries of intimate depictions of minors.¹⁷ While no court has squarely ruled on the issue of whether the First Amendment protects AI-generated sexual images of an identifiable child, it is hard to imagine a court ruling in the affirmative.

6. Arguments in support

According to the California District Attorneys Association:

California's prosecutors have long advocated for laws to strengthen protections for children, and our Legislature has heard our call in a variety of ways. For example, the statutes to be amended by AB 1946 were enacted to make it easier for victims to have disturbing images removed from social media platforms. Unfortunately, the statutes have not worked as hoped because social media corporations have found loopholes that allow them to ignore requests with impunity.

AB 1946 closes the loopholes by defining key terms, clarifying key provisions, and eliminating unnecessary barriers to removal such as the current provision that a social media platform receives complaints about a particular image "for four consecutive months" before they must act. (Civ. Code, § 3345.1, subd. (g)(4)(A).) This allows the corporation to knowingly leave CSAM images on the social media platform, available for viewing, for at least four months before making any effort to remove them.

AB 1946 also strengthens civil suit protections by permitting the Attorney General or a district attorney to file suit for violations rather than placing this burden on victims and their families.

7. Industry "concerns"

At the time this analysis was published, the Committee had not received opposition to this bill. The California Chamber of Commerce, CCIA, and TechNet have, however,

¹⁶ See *New York v. Ferber* (1982) 458 U.S. 747, 765 (CSAM not protected by the First Amendment); *Reno v. American Civil Liberties Union* (1997) 521 U.S. 844, 875 ("Sexual expression which is indecent but not obscene is protected by the First Amendment" (cleaned up)).

¹⁷ 47 U.S.C. § 223(h)(3).

submitted a letter setting forth their concerns with the bill. The issues they have flagged for concerns are set forth below, although they did not reach out directly to Committee staff or suggest amendments to resolve their concerns:

- The bill's requirement that a non-user be able to report CSAM on a platform.
- First and Fourth Amendment considerations; the letter states that these groups "want to carefully consider how changes requiring hash-matching, human-review, and changes to the enforcement in this bill affect [AB 1394's balancing of constitutional issues] as it relates to private-actor searches and state actor analyses under the Fourth Amendment."
- Expansion of the CSAM definition to include an individual who "reasonably appears to be a minor" and digital forgeries.
- The shortening of the compliance timeline.
- The bill's grant of regulatory authority to define "clear and conspicuous."
- The requirement to provide audits directly to the Attorney General and by request to public prosecutors.

SUPPORT

Children's Advocacy Institute at the University of San Diego School of Law (sponsor)
3Strands

California Family Council

California Coalition for Children's Safety and Health

California District Attorney's Association

California Institute for Technology & Democracy

Common Sense Media

Jewish Family and Children's Services

Organization for Social Media Safety

OPPOSITION

None received

RELATED LEGISLATION

Pending legislation:

AB 1705 (Bauer-Kahan, 2026) specifies that a pornographic website, as defined, has a duty of ordinary care to keep CSAM and nonconsensual sexual content off of its platform, and requires a pornographic website to obtain from a user specified information before the user can upload sexually explicit content. AB 1705 is pending before the Senate Privacy, Digital Technologies, and Consumer Protection Committee.

AB 2 (Lowenthal, 2025) 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.

Prior legislation:

AB 1137 (Krell, 2025) would have modified the social media CSAM reporting mechanism requirement established in AB 1397 (Wicks, Ch. 579, Stats. 2023). AB 1137 died in the Assembly Appropriations Committee.

AB 1394 (Wicks, Ch. 579, Stats. 2023) required a social media platform, as defined, to provide a mechanism for users to report CSAM in which they are depicted, and modified the enhanced civil remedy available to a minor who is the victim of sexual exploitation to include an enhanced civil remedy against a social media platform that facilitates or aids and abets commercial sexual exploitation of a minor, as defined. AB 1394 is discussed in further detail in Comment 3 of this analysis.

PRIOR VOTES

Assembly Floor (Ayes 75, Noes 0)

Assembly Appropriations Committee (Ayes 11, Noes 0)

Assembly Judiciary Committee (Ayes 12, Noes 0)

Assembly Privacy and Consumer Protection Committee (Ayes 14, Noes 1)
