**SENATE PRIVACY, DIGITAL TECHNOLOGIES, AND CONSUMER PROTECTION COMMITTEE**
**Senator Christopher Cabaldon, Chair**
**2025-2026 Regular Session**

AB 1946 (Wicks and Krell)
Version: May 21, 2026
Hearing Date: June 22, 2026
Fiscal: Yes
Urgency: No
BD

## SUBJECT

Reporting mechanism: child sexual abuse material.

## DIGEST

This bill updates and strengthens California's reporting mechanism for child sexual abuse material (CSAM) on social media.

## EXECUTIVE SUMMARY

CSAM is extremely pervasive on social media platforms, which are not only a popular place to spread CSAM but, in certain cases, can facilitate its creation. Once CSAM is uploaded or posted online, it can be circulated for years, leaving survivors to relive and experience this abuse far after it had originally occurred. Recognizing this issue, the Legislature passed 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. However, while groundbreaking, implementation reveals gaps in the accessibility, effectiveness, and accountability measures of the bill.

This bill addresses these implementation challenges 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. The bill also enhances the enforcement and accountability measures of AB 1394 by expanding enforcement to public prosecutors and requiring biannual audits to be submitted to the Attorney General to earn existing law's safe harbor, among other provisions.

This bill is sponsored by the Children's Advocacy Institute and is supported by a wide array of child safety and survivor advocacy groups, including Children Now and 3Strands Global Foundation. No timely opposition has been received, but a small coalition of industry groups, including TechNet, notes concerns. Should the bill pass out of this Committee, it will next be heard by the Senate Judiciary Committee.

## PROPOSED CHANGES TO THE LAW

Existing law:

1) 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. (47 U.S.C. § 223(h)(1).)

2) 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).)

3) Requires, not later than May 19, 2026, 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 provide 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 note.)

4) Requires online electronic service providers in the United States to report to the CyberTipline operated by the National Center for Missing & Exploited Children if they become aware of apparent CSAM on their platform. (18 U.S.C. § 2258A.)

5) Establishes criminal and civil penalties against perpetrators of sex trafficking and those who knowingly benefit from trafficking. (18 U.S.C. § 1591, 1595.)

6) Defines, among other terms:
   a) "Child abuse material" to include child pornography or obscene matter depicting a minor personally engaging in or personally simulating sexual conduct. Incorporates definitions from existing law, including:
      i. "Child pornography," which means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where any of the following apply:
         1) The production of such visual depiction involves the use of a minor engaging in sexually explicit conduct.
         2) 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.
         3) 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).)
      ii. "Minor," which means a person under the age of 18 years. (18 U.S.C. § 2256(8).)
      iii. "Obscene matter," which 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. (Pen. Code § 311)
   b) "Social media company" as a person or entity that owns or operates one or more social media platforms. (Bus. & Prof. Code § 22675)
   c) "Social media platform" as a public or semipublic internet-based service or application that has users in California and that meets both of the following criteria:

i. A substantial function of the service or application is to connect users in order to allow users to interact socially with each other within the service or application. A service or application that provides email or direct messaging services shall not be considered to meet this criterion on the basis of that function alone.
ii. The service or application allows users to do all the following:
    1) Construct a public or semipublic profile for purposes of signing into and using the service or application.
    2) Populate a list of other users with whom an individual shares a social connection within the system.
    3) Create or post content viewable by other users, including, but not limited to, on message boards, in chat rooms, or through a landing page or main feed that presents the user with content generated by other users. (Bus. & Prof. Code § 22675)

7) 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, but 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)

8) Makes a social media platform that fails to comply with the requirements described above liable to a reporting user for actual damages sustained by the reporting user

because of the violation, statutory damages of no more than $250,000, as specified, costs of the action, and any other relief the court deems proper. (Civ. Code § 3273.67)

9) Establishes a rebuttable presumption that the social media company is liable for statutory damages if it fails to comply with the reporting and blocking provisions described above within 60 days of the date on which the material was first reported. (Civ. Code § 3273.67)

10) Prohibits a social media platform from knowingly facilitating, aiding, or abetting commercial sexual exploitation of a minor or nonminor dependent. Deems a platform to have knowledge if CSAM is reported on its platform for four consecutive months, and provides that the platform is facilitating, aiding, or abetting if its features are a substantial factor in causing minor users to be victims of commercial sexual exploitation. Imposes statutory damages of between $1,000,000 and $4,000,000 for violations. (Civ. Code § 3345.1)

11) Provides that a platform is not subject to this liability if it institutes a program of at least biannual audits of its designs, algorithms, practices, affordances, or features that have the potential to result in violations; takes action within 30 days of completion of an audit designed to mitigate or eliminate foreseeable risk of violations; and provides the platform's board of directors with the audits within 90 days of completion of the mitigations. (Civ. Code § 3345.1)

This bill:

1) Changes and adds definitions to existing law, including:
    a) Replacing "obscene matter" in the definition of CSAM with "an intimate visual depiction involving an identifiable individual who is, or reasonably appears to be, a minor." Defines "intimate visual depiction" as one that depicts specified uncovered body parts of identifiable individuals, transfer of bodily fluids on to the body of identifiable individuals, or identifiable individuals engaging in sexually explicit conduct, as defined in existing Section 2256 of Title 18 of the United States Code.
    b) "Clear and conspicuous" means larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks, in a manner that clearly calls attention to the language.
    c) "Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice, as further defined by regulation.
    d) "Depicted individual" means a person who is depicted, including through the use of digitization or artificial intelligence, as a minor in child sexual abuse material on a social media platform.
    e) "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.

f) "Hash" means a unique, fixed-length alphanumeric value generated from the contents of an image.
g) "Hash-matching process" means a process by which images and videos of child sexual abuse material can be converted into hashes and used to identify known child sexual abuse material.
h) "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.

2) Removes the requirement that a reporting user is an identifiable minor in the reported material to report CSAM on a social media platform, effectively enabling all users to report.

3) Requires a social media platform to have its CSAM reporting mechanism be clear and conspicuous, not use dark patterns, and allow reporting for material sent or received through direct messaging systems.

4) Requires a social media platform to ensure that any report submitted through the reporting mechanism is reviewed through a hash-matching process.

5) Requires a social media platform to ensure that any report submitted through the reporting mechanism is reviewed by a natural person, if both of the following are true:
    a) There is no established or known hash match to child sexual abuse material with respect to the reported material.
    b) The reported material is not otherwise blocked.

6) Allows social media platforms to contact a reporting user by a method within the control of the social media company that owns or operates the platform, if the method is chosen by the reporting user and not under the influence of dark patterns.

7) Reduces the time that a social media platform has to complete the reporting process for CSAM from 30 days to 48 hours.

8) Reduces the time that a social media platform has to complete the reporting process, if circumstances beyond the reasonable control of the social media platform do not allow for a 48-hour compliance time, from 60 days to 5 days.

9) Requires the restoration of the availability or functionality of the reporting mechanism if the mechanism is unavailable or nonfunctional.

10) Subjects a social media company that fails to comply with Section 3273.66 of the Civil Code to a civil action brought by the Attorney General, a district attorney, a city attorney, or a county counsel for a civil penalty not to exceed $250,000 for each day that the reporting mechanism in violation of Section 3273.66 and for reasonable attorney's fees and costs.

11) Provides that a social media company shall not be liable for the above penalty if the social media company demonstrates, by clear and convincing evidence, that the violation was caused by circumstances beyond the social media company's control. Provides that penalties shall accrue daily until functionality of the reporting mechanism is restored and that the Attorney General, a district attorney, a city attorney, or a county counsel may seek injunctive relief to prevent ongoing violations.

12) Requires any penalty collected by the Attorney General, excluding reasonable attorney's fees and costs, to be deposited into the Survivor Support Fund.

13) Limits private standing to sue social media companies for failure to properly implement the CSAM reporting mechanism to depicted individuals who are reporting users, rather than reporting users generally. Enables depicted individuals who are not reporting users to obtain relief through an action filed by a parent, legal guardian, or other authorized representative for a platform's failure to block the material depicting the individual.

14) Requires that social media platforms submit biannual audits to the Attorney General and, if requested, to a district attorney, city attorney, or county counsel to achieve safe harbor from knowingly facilitating, aiding, or abetting commercial sexual exploitation of a minor or nonminor dependent.

15) Removes the requirement that material was reported using the CSAM reporting mechanism for four consecutive months to have knowledge of facilitating, aiding, and abetting commercial sexual exploitation of a minor or nonminor dependent.

## COMMENTS

1. CSAM on social media

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.[1]

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.[2]

As alluded to by NCMEC, while CSAM can include printed materials, CSAM is largely created and spread via technology.[3] Tragically, the creation and trading of CSAM is extremely pervasive on the Internet, especially in the United States. According to the Internet Watch Foundation (IWF), the United States hosted 16 percent of the world's webpages that depicted or led to CSAM.[4] This was the second most in the world, with a

---

[1] *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.
[2] *Child Sexual Abuse Material Overview* (2018) National Center for Missing & Exploited Children, https://ncmec.org/theissues/csam.
[3] O'Brien et al., *"They are not victimless crimes… that's frustrating to hear": Qualitative insights from prosecutors working on cases related to technology facilitated child sexual abuse material* (January 1, 2025) Child Abuse & Neglect, 159, https://www.sciencedirect.com/science/article/abs/pii/S0145213424005623?via%3Dihub.
[4] *Geographic Insights* (2025). Internet Watch Foundation, https://www.iwf.org.uk/annual-data-insights-report-2025/online-hosting/geographic-insights/.

staggering total of 54,343 URLs.[5] Once a child sexual abuse image is shared on the internet, it can be nigh impossible to remove due to its rapid circulation. For instance, NCMEC noted in their 2025 CyberTipline Report that one individual had their CSAM spread for the past 20 years, appearing in more than 1.4 million takedown submissions to the nonprofit.[6]

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.[7] 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.[8] 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:

> 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.[9]

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

---

[5] *Ibid*.
[6] *2025 CyberTipline Report* (2026) National Center for Missing & Exploited Children, https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata.
[7] *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.
[8] *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.
[9] 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.

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.[10] More than 1.1 million of these reports related to CSAM detection in AI training datasets.

School districts worldwide are experiencing this firsthand in several horrifying ways. In Utah, for example, an elementary school employee allegedly photographed students without their knowledge to later turn the photos into GenAI CSAM.[11] In the United Kingdom, the IWF reported that a secondary school was blackmailed by criminals who took photos of students from the school's website and transformed them into GenAI CSAM.[12] Across the United States, students themselves are creating GenAI CSAM of their classmates. As noted by the New York Times:

> Boys in several states have used widely available "nudification" apps to pervert real, identifiable photos of their clothed female classmates, shown attending events like school proms, into graphic, convincing-looking images of the girls with exposed A.I.-generated breasts and genitalia. In some cases, boys shared the faked images in the school lunchroom, on the school bus or through group chats on platforms like Snapchat and Instagram, according to school and police reports.
>
> Such digitally altered images — known as "deepfakes" or "deepnudes" — can have devastating consequences. Child sexual exploitation experts say the use of nonconsensual, A.I.-generated images to harass, humiliate and bully young women can harm their mental health, reputations and physical safety as well as pose risks to their college and career prospects. Last month, the Federal Bureau of Investigation warned that it is illegal to distribute computer-generated child sexual abuse material, including realistic-looking A.I.-generated images of identifiable minors engaging in sexually explicit conduct.[13]

2. Legislative history: AB 1394, AB 1137, and the TAKE IT DOWN Act

To address the issue of CSAM on social media, the Legislature passed AB 1394 (Wicks, Ch. 579, Stats. 2023), which established a revolutionary framework for social media users to report CSAM. Specifically, AB 1394 imposed two primary obligations:

---

[10] *2025 CyberTipline Report* (2026) National Center for Missing & Exploited Children, https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata.
[11] Pat Reavy, *Utah school employee took photos of students, created child sex abuse material, policy say* (May 15, 2026) KSL, https://www.ksl.com/article/51498180/utah-school-employee-took-photos-of-students-created-child-sex-abuse-material-police-say.
[12] Dan 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.
[13] Natasha Singer, *Teen Girls Confront an Epidemic of Deepfake Nudes in Schools* (April 8, 2024) New York Times, https://www.nytimes.com/2024/04/08/technology/deepfake-ai-nudes-westfield-high-school.html.

1) CSAM Reporting and Removal: Social media platforms must provide a mechanism for users to report material they reasonably believe constitutes CSAM in which they are depicted as identifiable minors. The platform must review, block, and remove the reported content within 30 days (extendable to 60 days in limited circumstances) and issue written confirmation and weekly status updates to the reporting user. Platforms are required to block not only the reported material but also to make reasonable efforts to prevent the recirculation of the same content.

2) Liability for Facilitating Commercial Sexual Exploitation: The bill amended Civil Code Section 3345.1 to impose civil liability—ranging from $1 million to $4 million per act—on social media platforms that knowingly "facilitate, aid, or abet" the commercial sexual exploitation of minors. "Facilitate, aid, or abet" was defined to include deploying a system, design, feature, or affordance that is a substantial factor in causing exploitation. Platforms could invoke a safe harbor if they conducted biannual audits that were sent to the platform's board of directors and mitigated foreseeable risks.

AB 1934 became operative in 2025. While AB 1394 marked an important step in addressing the proliferation of CSAM on social media, its implementation reveals various gaps and shortcomings. To begin, to submit a report, AB 1394 requires that the user reasonably believe that they are an identifiable minor depicted in CSAM. This effectively restricts who is allowed to use the reporting mechanism to survivors in CSAM. Social media platforms are under no obligation to allow parents, guardians, teachers, or any other user, for that matter, to use the comprehensive reporting mechanism. Considering that, oftentimes, survivors may be fully unaware that their CSAM is being spread online, much less have access to all the various social media platforms, this significantly limits the effectiveness of existing law.

Secondly, social media platforms are under no obligation to meaningfully review reported material. While platforms may employ whatever technological tools or review processes they deem fit, there is no set standard for how much scrutiny a report must be under. This can lead to significant consequences for survivors, as a platform may not scrutinize a CSAM report, causing it to remain online.

Additionally, the author and supporters note that, currently, some platforms make it difficult to locate the reporting mechanism altogether. As noted by the Children's Advocacy Institute, the bill's sponsor:

> [A] report released in August 2025 by the Children's Advocacy Institute (CAI) at the University of San Diego School of Law, Child Cruelty by Design, details how the world's largest social media platforms — including Meta, TikTok, and Snap — use confusing, multi-step, and

inaccessible reporting systems that make it intentionally hard for users to report CSAM, sexual exploitation, and other violations.

In part, CAI's Child Cruelty by Design report analyzed whether social media platforms' reporting systems met the requirements of AB 1394 (Wicks and Flora) (Chapter 579, Statutes of 2023) and SB 1504 (Stern) (Chapter 900, Statutes of 2024), which mandate that tools for reporting CSAM and other harmful content be reasonably accessible and prominently displayed. CAI's research determined that none of the platforms met those standards, citing:

- Multiple, confusing steps to locate and submit reports.
- Vague or misleading labels that obscure how to report CSAM or exploitation.
- Interfaces ill-suited for mobile users, despite most youth accessing platforms via smartphones.

Furthermore, while AB 1394 provided a private right of action for reporting users who are depicted in CSAM, AB 1394 was silent about public enforcement. While generally, the Attorney General retains the authority to enforce all California laws, AB 1394 did not specify that public prosecutors could enforce its provisions.

Lastly, the safe harbor provision of AB 1394 allows social media platforms to evade liability for knowingly facilitating, aiding, or abetting commercial sexual exploitation if a platform 1) conducts biannual audits, 2) sends those audits to its board of directors, and 3) mitigates foreseeable risks identified by the audits. However, there is no independent or external check on whether these audits are being done in a comprehensive or meaningful way. As such, platforms may self-certify compliance without any real scrutiny.

Last year, AB 1137 (Krell, 2025) would have made several similar changes to this bill to address these aforementioned concerns. Among these changes were expanding reporting to all users, authorizing public enforcement, increasing the reporting mechanism's accessibility, and strengthening the safe harbor provision. AB 1137, however, was held in the Assembly Appropriations Committee.

Additionally, the federal TAKE IT DOWN Act (TIDA), passed in 2025, provides that various online platforms create a process by which a survivor or their authorized representative can request the removal of their nonconsensual intimate imagery. TIDA also requires online platforms to remove this imagery within 48 hours of a survivor's valid request, providing an expedited timeline when compared to AB 1394's 30-day timeline.

3. What this bill does

This bill seeks to strengthen and improve AB 1394. To do this, the bill takes several provisions from AB 1137 and draws inspiration from TIDA. Firstly, this bill strengthens AB 1394's reporting mechanism in multiple ways. Chief among these is that this bill expands the ability to report to all users. The bill further provides several improved accessibility features, including specifying that the reporting mechanism be clear and conspicuous, not use dark patterns, and enable reporting through direct messaging systems. Seeking alignment with TIDA, this bill changes many of the definitions in existing law to the definitions used in TIDA and reduces the timeline to complete the reporting process from 30 days to 48 hours, subject to certain exemptions. The bill additionally adds a strengthened review process by requiring that reports be reviewed by a hash-matching process and, in certain circumstances, by a natural person. Taken holistically, these changes should provide California with a greatly improved mechanism to further combat CSAM on social media.

This bill also seeks to strengthen the enforcement and accountability measures of AB 1304. To achieve this objective, this bill requires that the biannual audits be sent to the Attorney General and provided to public prosecutors, upon request, to achieve existing law's safe harbor. It also provides robust public enforcement, with penalties of $250,000 per day for noncompliance, with any penalty collected by the Attorney General to be deposited in the Survivor Support Fund. Accordingly, since the bill expands who can report, this bill modifies the private right of action to ensure that it remains intact and the same as AB 1394. Lastly, this bill eliminates the four-month requirement in the knowledge standard.

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.

4. Policy Consideration

While this bill shortens the timeline a social media platform has to complete the reporting process to 48 hours, it leaves some timeline provisions of existing law untouched. Namely, the bill requires written updates to be provided seven days after providing written confirmation to the user, and requires social media platforms to provide said written confirmation 36 hours after the material was first reported. Evidently, these timelines do not align with the bill's 48-hour requirement to complete the entire reporting process. Moving forward, the author may wish to adjust these timelines with the bill's other provisions to ensure consistency.

5. Stakeholder Positions

The California District Attorneys Association writes in support:

> 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.
>
> Like you, we believe social media platforms should remove CSAM when they become aware of its existence on their sites and should be held accountable when they do not.

Children Now makes the case:

> The harms inflicted by CSAM are not fleeting; they are lifelong. Once abusive images are shared online, they can circulate indefinitely, subjecting survivors to ongoing revictimization with every viewing. AB 1946 is a meaningful commitment to ensuring resources reach vulnerable children and youth.

While they have not submitted formal opposition, a coalition of industry groups, consisting of TechNet, California Chamber of Commerce, and Computer & Communications Industry Association, writes in concern:

> We will highlight a few issues that warrant additional discussion and potential amendments.
>
> - Expansion of access to the reporting mechanism in 3273.66 to all users. While many platforms already allow all users to report CSAM, we want to consider how this expansion interacts with

other provisions in the bill and current law to minimize unintended consequences.

- First and Fourth Amendment considerations. AB 1394 struck a careful, but tenuous balance regarding constitutional issues related to the free speech protections of the First Amendment and the protections against warrantless searches in the Fourth Amendment. We want to carefully consider how changes requiring hash-matching, human-review, and changes to the enforcement in this bill affect that balance as it relates to private-actor searches and state actor analyses under the Fourth Amendment. The last thing TechNet, our coalition, or our members want is for a criminal defendant to be able to overturn their conviction based on evidence collected as a result of this bill.
- Expansion of the definition of "child sexual abuse material" to include an individual who "reasonably appears to be a minor" and digital forgeries
- Changes to the compliance timeline from 30 days to 48 hours will likely have significant unintended consequences and also confusion as to which timeframe is controlling.
- Regulatory authority for the Attorney General to define "clear and conspicuous", which is well-defined in BPC 17601.
- Providing audits directly to the Attorney General and by request to public prosecutors.

**SUPPORT**

Children's Advocacy Institute (Sponsor)
3Strands Global Foundation
Bright Light Strategies
California Coalition for Children's Safety and Health
California District Attorneys Association
California Family Council
California Initiative for Technology & Democracy, a Project of California Common CAUSE
Children Now
Jewish Family and Children's Services of San Francisco, the Peninsula, Marin and Sonoma Counties
Organization for Social Media Safety
2 Individuals

**OPPOSITION**

None received.

## RELATED LEGISLATION

AB 1705 (Bauer-Kahan, 2026) would require operators of pornographic internet websites to exercise ordinary care and reasonable diligence to ensure that sexually explicit content is not displayed on their websites and would require operators to take reasonable steps to ensure that sexually explicit content does not include an individual who did not consent or was a minor when the content was created. AB 1705 is pending before the Senate Judiciary Committee.

AB 392 (Dixon, 2025) was substantially similar to AB 1705. AB 392 died in the Senate Appropriations Committee.

AB 1137 (Krell, 2025) *See* Comment 2.

SB 646 (Cortese, 2024) would have allowed a person who is depicted in certain sexual images when the person was less than 18 years of age to bring a civil action for specified relief against a person or entity that distributes that material, as specified; and would have required the operator of an online service or website to list an agent for notification of claimed violation of the provisions related to CSAM, as specified. SB 646 died in the Assembly Appropriations Committee.

AB 1394 (Wicks, Ch. 579, Stats. 2023) *See* Comment 2.

SB 1056 (Umberg, Ch. 881, Stats. 2022) required a social media platform, as defined, to clearly and conspicuously state whether it has a mechanism for reporting violent posts, as defined; and allowed a person who is the target, or who believes they are the target, of a violent post to seek an injunction to have the violent post removed.

AB 602 (Berman, Ch. 491, Stats. 2019) allows a person who is depicted in nonconsensual deepfake pornography to bring a civil action for damages against a person who intentionally creates or distributes the material.

## 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)

**********