Date of Hearing: April 16, 2026
Fiscal: Yes

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
AB 1946 (Wicks) – As Amended April 6, 2026

SUBJECT: Reporting mechanism: child sexual abuse material

SYNOPSIS

Child sexual abuse material, commonly referred to under the acronym "CSAM," is tragically pervasive on the internet – not only in its illicit corners, on the so-called "dark web," but also on popular social media websites and applications that billions of people use each day. This tragedy is compounded by the fact that certain websites and applications are not only a convenient means for sharing CSAM but arguably facilitate its production.

AB 1394 (Wicks, Flora; Stats. 2023, Ch. 579) requires social media platforms to provide a mechanism for users to report CSAM in which they are depicted, and subjects platforms to liability if they fail to comply with these requirements or knowingly facilitate, aid, or abet commercial sexual exploitation. The bill also includes a safe harbor for platforms that opt to undertake biannual audits sent to the platform's Board of Directors.

Last year's AB 1137 (Krell) would have updated and strengthened AB 1394 by expanding reporting and accountability provisions under that law. The bill also required a natural person review reported material if there is no established or known hash match or if the material is not otherwise blocked. That bill passed this Committee on a 13-0 vote but was held in the Appropriations Committee. This author-sponsored bill incorporates many of the provisions from AB 1137 and seeks to align AB 1394 with the federal TAKE IT DOWN ACT, including by expediting compliance timelines. The bill also requires that the biannual audits be submitted to the Attorney General, and if requested, to a local public prosecutor.

The bill is sponsored by the Children's Advocacy Institute of the University of San Diego School of Law and is supported by, among others, 3Strands Global Foundation, Fairplay, and the Organization for Social Media Safety. The bill has no registered opposition; however, TechNet, California Chamber of Commerce, and Computer & Communications Industry Association have taken a "concerns" position.

If passed by this Committee, this bill will next be heard by the Judiciary Committee.

EXISTING LAW:

1) 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.)

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

3) Makes it a federal crime to knowingly share or threaten to share such images and requires websites and online platforms to remove the images within 48 hours of receiving a survivor's verified request. (Pub. L. 119-12.)

4) 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. (*Id.* at (1).).

        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(a).)

    b. "Social media company" as a person or entity that owns or operates one or more social media platforms. (Bus. & Prof. Code § 22675(e).)

    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(f).)

5) Requires a social media platform to do all the following:

   a. Provide an accessible mechanism for California users to report material to the platform the user reasonably believes is CSAM that is displayed, stored, or hosted on the platform. (Civ. Code § 3273.66(a).)

   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. (*Id.* at (b), (c).)

   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, hosted on the platform; and the report contains basic identifying information sufficient to permit the platform to locate the reported material. (*Id.* at (d).)

   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. (*Id.* at (e).)

   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. (*Id.* at (f).)

   f. Issue a final written determination to the reporting use stating whether the material has been determined to be CSAM displayed, stored, or hosted on the social media platform. (*Id.* at (g).)

   g. Comply with the requirements described above within 30 days unless there are circumstances beyond the reasonable control of the platform, 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. (*Id.* at (h).)

6) 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(a).)

7) 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. (*Id.* at (b).)

8) 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 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. 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(g).)

THIS BILL:

1) Changes and adds definitions to AB 1394, 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" has the same meaning as provided in existing Business and Professions Code section 17601: 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" has the same meaning as provided in existing Civil Code section 1798.140: 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) Requires CSAM reporting mechanisms on social media platforms to be clear and conspicuous, refrain from dark patterns, and apply to material sent or received through direct messaging systems.

3) Expands the scope of users who may report CSAM to a social media platform by no longer limiting such users to identifiable minors, thereby enabling any user to submit such reports.

4) Requires platforms to ensure CSAM reports are reviewed by a natural person if the material does not match a hash value for known CSAM and will not otherwise be blocked.

5) Removes the requirement that the method by which a social media platform must contact a reporting user not be within the platform's control.

6) Shortens the timelines for blocking CSAM and providing written communications to the reporting user to 48 hours, unless extenuating circumstances apply, in which case the timeframe is extended to five days.

7) Subjects a social media company to a civil action brought by a public prosecutor for a civil penalty not to exceed $250,000 for each day that the reporting mechanism is unavailable or nonfunctional. Prevailing public prosecutors may also receive reasonable attorney's fees and costs.

8) Provides an exemption from liability for an unavailable or nonfunctional reporting mechanism, as specified, if the social media company demonstrates, by clear and convincing evidence, that the unavailability or non-functionality was caused solely by circumstances beyond the social media company's reasonable control, as specified. Specifies that penalties accrue daily and enables public prosecutors to seek injunctive relief as necessary to prevent ongoing violations.

9) Requires that any penalty collected by the Attorney General, less reasonable attorney's fees and costs, be deposited into the Survivor Support Fund established pursuant to Section 647.5 of the Penal Code.

10) 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 for a platform's failure to block the material depicting the individual.

11) Provides that biannual audits under that provision must be submitted to the AG, and if requested, to a local public prosecutor.

COMMENTS:

1) **Author's statement**. 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) **Background**. Child sexual abuse material, commonly referred to under the acronym "CSAM," is tragically pervasive on the internet. Roughly 500 CSAM files are traded online every minute.[1] From 2013 to 2023, the number of CyberTipline reports received by the National Center for Missing & Exploited Children (NCMEC), a federally-chartered nonprofit, skyrocketed from 500,000 to over 36 million.[2] The scourge of CSAM exists not only in the illicit corners of the internet, on the so-called "dark web," but also on popular social media websites and applications that billions of people use every day. However, reports dropped 19% in 2024, a decline almost entirely attributable to Meta – the Facebook, Instagram, and WhatsApp parent company that submits roughly two-thirds of the reports – as a result of the company's adoption of end-to-end encryption on Facebook and Messenger, a practice that increases security and privacy but also can allow sex traffickers to operate undetected.[3] According to NCMEC, "[t]his decline is especially concerning because the REPORT Act, which was enacted in 2024, mandates companies report two additional forms of child sexual exploitation for the first time – child sex trafficking and online enticement."[4]

Compounding the tragic prevalence of CSAM online, many of these websites and applications are not only a convenient means for sharing CSAM but also provide features that facilitate its production. For example, "[a] *Forbes* review of hundreds of recent TikTok livestreams reveals how viewers regularly use the comments to urge young girls to perform acts that appear to toe the line of child pornography—rewarding those who oblige with TikTok gifts, which can be redeemed for money, or off-platform payments to Venmo, PayPal or Cash App accounts that users list in their TikTok profiles."[5] In other cases, platforms are culpably inattentive, such as

---

[1] Jessica McGarvie, "From Hashtag to Hash Value: Using the Hash Value Model to Report Child Sex Abuse Material," 13 Seattle Journal of Environmental Law (2023) 1, 1.
[2] 2023 CyberTipline Report, https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata.
[3] Ben Goggin, "Child exploitation watchdog says Meta encryption led to sharp decrease in tips and reports" *NBC News* (May 8, 2025), https://www.nbcnews.com/tech/security/child-exploitation-watchdog-says-meta-encryption-led-sharp-decrease-ti-rcna205548. The reduced figure accounts for Meta's new practice of "bundling" related reports.
[4] 2024 CyberTipline Report, https://ncmec.org/gethelpnow/cybertipline/cybertiplinedata.
[5] Levine, "How TikTok Live Became 'A Strip Club Filled With 15-Year-Olds,'" *Forbes* (Apr. 27, 2022), https://www.forbes.com/sites/alexandralevine/2022/04/27/how-tiktok-live-became-a-strip-club-filled-with-15-year-olds/. For more examples, see e.g. Asia Grace, "'So f-ked up': Instagram slammed for allowing paid content

Meta's alleged former policy of allowing 17 strikes before it suspended accounts engaged in sex-trafficking.[6]

Under federal law, online electronic service providers (ESPs) in the United States must report to the CyberTipline operated by NCMEC if they become aware of apparent CSAM on their platform. Using the geolocation provided by the ESPs, NCMEC reviews and refers the reports to relevant law enforcement agencies.[7] ESPs may, but are not required to, use NCMEC's Take It Down tool, which is funded by Meta. The tool "works by assigning a unique digital fingerprint, called a hash value, to nude, partially nude, or sexually explicit images or videos of people under the age of 18. Online platforms can use hash values to detect these images or videos on their services and remove this content."[8] Once a hash is generated, social media platforms can use it to not only remove existing copies of the CSAM, but also rapidly compare image and video files that users attempt to upload for a match, analogous to the process that they use to scan incoming files for computer viruses.

Artificial intelligence can exacerbate and mitigate the proliferation of CSAM. As numerous state Attorneys General – California's Rob Bonta included – have recently written, the urgency and ubiquity of these problems are increasing due to the widespread availability of generative AI, which can be used to create sexual deepfakes.[9] NCMEC's CyberTipline saw a 1,325% increase in reports involving Generative AI, going from 4,700 in 2023 to 67,000 reports in 2024.[10] On the other hand, some platforms, such as Google and Meta, are using machine learning algorithms to identify potentially harmful content more efficiently.[11]

3) **AB 1394 (Wicks)**. To ensure social media platform accountability when users report CSAM, AB 1394 (Wicks, Flora; Stats. 2023, Ch. 579), which became operative January 1, 2025, requires platforms to establish a mechanism for underage users to report suspected CSAM they are depicted in and requires the platforms to permanently block CSAM and update the user who reported the violation throughout the process, which generally must be completed within 30 days of the report. Platforms that violate these provisions are subject to civil liability, including actual damages to the reporting user and statutory damages of up to $250,000 per violation.

---

featuring kids in bikinis," *New York Post* (Nov. 2, 2022), https://nypost.com/2022/11/02/instagram-slammed-for-paid-content-featuring-kids-in-bikinis; Jeff Horwitz and Katherine Blunt, "Instagram Connects Vast Pedophile Network," *The Wall Street Journal* (Jun. 7, 2023), https://www.wsj.com/articles/instagram-vast-pedophile-network-4ab7189; Jennifer Valentino-DeVries and Michael H. Keller, "She Was a Child Instagram Influencer. Her Fans Were Grown Men," *The New York Times* (Nov. 10, 2024), https://www.nytimes.com/2024/11/10/us/child-influencer.html.

[6] Jonathan Limehouse, "Meta had 17-strikes policy for sex trafficking posts, lawsuit alleges," *USA Today* (Nov. 22, 2025), https://www.usatoday.com/story/tech/2025/11/22/meta-strike-policy-sex-trafficking-violations-testimony/87425612007/.

[7] Paul Bischoff, "The rising tide of child abuse content on social media," *Comparitech* (Jul. 9, 2024) https://www.comparitech.com/blog/vpn-privacy/child-abuse-online-statistics/.

[8] NCMEC: Take It Down, available at https://takeitdown.ncmec.org/.

[9] "Artificial Intelligence and the Exploitation of Children," National Association of Attorneys General (Sept. 5, 2023), https://ncdoj.gov/wp-content/uploads/2023/09/54-State-AGs-Urge-Study-of-AI-and-Harmful-Impacts-on-Children.pdf.

[10] 2024 CyberTipline Report, https://ncmec.org/gethelpnow/cybertipline/cybertiplinedata.

[11] Paul Bischoff, "The rising tide of child abuse content on social media" *Comparitech* (Jul. 9, 2024) https://www.comparitech.com/blog/vpn-privacy/child-abuse-online-statistics/.

AB 1394 also prohibits social media platforms from knowingly facilitating, aiding, or abetting commercial sexual exploitation of minors. "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. Each violation subjects the platform to statutory damages of up to $4,000,000 but no less than $1,000,000. The bill delineates circumstances in which a platform is deemed to have knowledge and provides a safe harbor from this liability where the platform has undertaken biannual audits and corrected its designs, algorithms, practices, affordances, and features that pose a risk of a violation, as specified.

4) **What this bill would do.** Last year's AB 1137 (Krell) would have updated and strengthened AB 1394 by expanding reporting and accountability provisions under that law. The bill passed this Committee on a 13-0 vote but was held in the Appropriations Committee.

In April 2025, Congress passed the TAKE IT DOWN Act to combat the spread of nonconsensual intimate imagery of real people. The Act makes it a federal crime to knowingly share or threaten to share such images and requires websites and online platforms to remove the images within 48 hours of receiving a survivor's verified request.

This bill incorporates many of the provisions from AB 1137 and seeks to existing law with the TAKE IT DOWN ACT. Specifically, the bill:

- Requires the reporting mechanism to be clear and conspicuous and prohibits the use of dark patterns.

- Aligns definitions with the TAKE IT DOWN Act and expedites the timeline for social media companies to block reported CSAM to generally align with the 48-hour timeline established that Act. In extenuating circumstances, the timeline may be extended to five days.

- Expands the scope of users who may report CSAM to a social media platform by no longer limiting such users to identifiable minors, thereby enabling any user to submit such reports.

- Requires platforms to ensure CSAM reports are reviewed by a natural person if the material does not match a hash value for known CSAM and will not otherwise be blocked.

- Subjects a social media company to a civil action brought by a public prosecutor for a civil penalty not to exceed $250,000 for each day that the reporting mechanism is unavailable or nonfunctional, unless the social media company demonstrates, by clear and convincing evidence, that the unavailability or non-functionality was caused solely by circumstances beyond the social media company's reasonable control, as specified.

- Enables depicted individuals who are not reporting users to obtain relief for a platform's failure to block the material depicting the individual.

- Provides that biannual audits must be submitted to the AG, and if requested, to a local public prosecutor.

5) **Concerns**. TechNet, California Chamber of Commerce, and Computer & Communications Industry Association, taking a "concerns" position, highlight the following issues:

- 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.

ARGUMENTS IN SUPPORT: The bill's sponsor, the Children's Advocacy Institute of the University of San Diego School of Law, writes:

> We should not need to pass laws to compel platforms to do any of this. Any business behaving with even a molecule of morality would not evade their obligations to aid suffering, sexually abused children.
>
> And yet, here we are – again. That we must resort to bills like this one tells you everything you need to know about why AB 1946 is necessary to protect our most horribly exploited children from just a handful of unimaginably wealthy corporations that could do far more to help them, but don't.

The Organization for Social Media Safety writes:

> The proliferation of social media platforms has created new and evolving challenges in addressing child harm and exploitation. California has responded by enacting laws requiring social media platforms to establish and maintain mechanisms through which users can report child-endangering material. Yet these protections are only meaningful if the reporting systems are genuinely accessible. Too often, platforms either fail to comply with the spirit and letter of these laws or exploit gaps and ambiguities in ways that frustrate their child-protective purpose.

This implementation problem is not hypothetical. AB 2481, authored by Assemblymember Lowenthal and sponsored by the Organization for Social Media Safety, created a verified reporter process for school leaders and licensed mental health professionals and became effective on January 1, 2026. Yet today, nearly all the platforms subject to that law still do not appear to be providing the required reporting pathways in a compliant and usable manner. That experience reinforces a central lesson: platform reporting obligations must be clear, modernized, and backed by stronger accountability measures if they are to protect children in practice.

REGISTERED SUPPORT / OPPOSITION:

Support

Childrens Advocacy Institute (Sponsor)
3strands Global Foundation
Fairplay
Fred Whitaker
Organization for Social Media Safety
Richard Freed
2 Individuals

Opposition

None on file.

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