Date of Hearing: April 22, 2025
Fiscal: Yes

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
AB 1137 (Krell) – As Amended April 21, 2025

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—and 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 induce 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.

This bill updates and strengthens AB 1394 by, among other things, enabling any user to report CSAM, granting public prosecutors enhanced civil enforcement authority to hold accountable platforms that fail to maintain a properly functioning reporting mechanism, and requiring the aforementioned audits to be conducted by independent third-party auditors and made public, with redactions for trade secrets.

The bill is sponsored by the Children's Advocacy Institute at the University of San Diego School of Law and National Center on Sexual Exploitation, and is supported by the California Initiative for Technology & Democracy (CITED), Jewish Family and Children's Services in the in the Bay Area, and the National Center for Missing & Exploited Children.

The bill is opposed by TechNet, California Chamber of Commerce, and Computer & Communications Industry Association.

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

THIS BILL:

1) Requires CSAM reporting mechanisms on social media platforms to be clear and conspicuous.

2) 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.

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

4) Enables public prosecutors to bring a civil action against a social media company for each day the mechanism is unavailable or nonfunctional. The public prosecutor may seek up to $250,000 for each day in which the company is noncompliant, as well as reasonable attorney's fees and costs. Deems a mechanism unavailable or nonfunctional if the mechanism is inaccessible or otherwise not compliant with existing requirements governing the mechanism. Enables the Attorney General to seek injunctive relief to compel a social media company to immediately restore and maintain a fully functional reporting mechanism.

5) 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.

6) With respect to an existing provision that shields social media platforms from liability for knowing facilitation, aiding, or abetting of commercial sexual exploitation if they conduct biannual audits, requires that such audits be conducted by independent third-party auditors with proven experience in trust and safety and content moderation. The audit must be made public within 90 days of completion, and may be redacted for trade secrets.

7) Clarifies that definition of "facilitate, aid, or abet" applies to commercial sexual exploitation of minors, rather than minor users.

8) Contains a severability clause.

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) 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. "Clear and conspicuous" to mean 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. (Bus. & Prof. Code § 17601.)

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

d. "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 of 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).)

3) Requires a social media platform to do all of 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).)

4) 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 as a result 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).)

5) 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).)

6) 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 a 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).)

COMMENTS:

1) **Author's statement**. According to the author:

> Social media has become one of the preferred avenues for predators to solicit, market, and share child sexual abuse material (CSAM). In 2023 alone, Facebook and Instagram each reported more than 10,000,000 instances of CSAM, as noted in the CyberTipline Reports by Electronic Services Providers. Behind the reports are images of kids who have been sexually abused. The most frequently traded CSAM depicts children aged 9-12 years old. In graphic and brutal pictures and videos, the violation of a child is on display for the world to see. For the child, it serves as a permanent reminder of their trauma and humiliation.
>
> AB 1137 strengthens the existing tool to report child sexual abuse material on social media platforms by allowing anyone to report CSAM (not just the victim depicted), requiring reports to be reviewed by a natural person, and empowering victims to take legal action. This bill further compels social media platforms to have more transparency by requiring the reporting mechanism to be clear and conspicuous.
>
> Existing law allows social media companies to be protected from liability for commercial sexual exploitation if they conduct a biannual audit aimed at identifying designs and features contributing to its spread. To improve transparency and accountability, this bill would instead require that audit to be performed by a third-party and made public.

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. Last year, Discord, TikTok, and the platform formerly known as Twitter submitted hundreds of thousands of reports; Google reported nearly 1.6 million; and Meta – the parent company of Facebook, Instagram, and WhatsApp – submitted more than 30.5 million reports across those platforms.[3]

This tragedy is compounded by the fact that certain websites and applications are not only a convenient means for sharing CSAM, but arguably induce 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."[4]

---

[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] CyberTipline 2023 Report, https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata.
[3] https://www.missingkids.org/content/dam/missingkids/pdfs/2023-reports-by-esp.pdf
[4] 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 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

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.[5] However, NCMEC reports that in 2023 it "continued to see inconsistencies in reporting from electronic service providers and tech companies regarding exploitation on their platforms. The majority of companies did not report at all, and many reports did not include the necessary details for NCMEC or law enforcement to take action."[6]

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."[7] 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.

In support of the bill, NCMEC writes:

> In NCMEC's experience CSAM often recirculates on the Internet long after a child's initial physical abuse. This causes severe harm, psychological impact, and physical safety concerns for child victims, and adult survivors of these crimes, as offenders redistribute sexually exploitative material and track, harass, and share personal information relating to child victims. For many victims, one of their primary goals is to ensure that CSAM images and videos in which they are depicted are removed from the Internet as quickly as possible and stop circulating online. While NCMEC operates a notice and takedown program to notify online platforms when we receive a report of apparent CSAM, our notices do not have the force of law, and most platforms take days to remove content or do not respond at all to NCMEC's notices.

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.[8] On the other hand, some platforms, such as Google and Meta, are using machine learning algorithms to identify potentially harmful content more efficiently.[9]

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.

[5] 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/.

[6] *NCMEC 2023 CyberTipline Report* (2024), p.3 https://www.missingkids.org/content/dam/missingkids/pdfs/2023-CyberTipline-Report.pdf.

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

[8] "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.

[9] 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/.

3) **AB 1394**. To ensure social media platform accountability when users report CSAM, AB 1394, 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.

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 post a risk of a violation, as specified.

4) **What this bill would do.** This bill updates and strengthens AB 1394 by:

- Requiring the reporting mechanism to be clear and conspicuous.

- Enabling any user to submit reports of CSAM. Current law limits reporting users to victims, restricting the reach of AB 1394. Just as anyone can report child abuse offline, it makes sense to ensure any user of the platform can report CSAM.

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

- Enabling public prosecutors to bring a civil action against a social media company for each day the mechanism is unavailable or nonfunctional. The public prosecutor may seek a civil penalty of up to $250,000 per day and reasonable attorney's fees and costs. Additionally, the AG may seek injunctive relief to compel a social media company to restore and maintain a fully functional reporting mechanism. This ensures that accountability for properly implementing a mechanism does not fall on the shoulders of those depicted in CSAM. Granting enforcement to public prosecutors only is intended to assuage concerns about excessive litigation.

- Enabling a depicted individual who is not a reporting user to obtain relief for a platform's failure to block content containing the individual. An individual's status as the reporter of the CSAM is immaterial to the harm they may suffer as a result of a platform's failure to block the CSAM.

- With respect to the existing provision that shields social media platforms from liability for knowing facilitation of commercial sexual exploitation if they conduct biannual audits, the bill requires that such audits must be conducted by independent third-party auditors and made public within 90 days of completion, but allows for trade secret redactions. Proponents argue that if social media companies are to be provided a safe harbor, transparency is a fair trade-off.

In support of the bill, NCMEC writes:

> AB 1137 will expand access to justice for child victims and clarify the obligations of social media platforms to remove CSAM they are displaying, storing, or hosting. The bill will require social media platforms to conduct a human review of reported material if there is no hash match to a known CSAM image. This will ensure that material reported by child victims is thoroughly reviewed and actioned by the platform and that platforms are fully engaged in the reporting process.
>
> The bill also will enhance accountability and transparency requirements for social media platforms by requiring that an experienced subject matter expert audit their designs, algorithms, and features and that these audit reports be made available not only to the platform's Board of Directors, but also to the public. NCMEC applauds AB 1137's requirement that platforms utilize an expert with experience in trust and safety and content moderation issues to ensure that the audit is substantive and focuses on relevant aspects of technology and offender behavior online.
>
> Crucially, AB 1137 will empower the California Attorney General and state and local prosecutors to protect child victims in California by enabling civil actions and actions for injunctive relief against social media platforms that fail to comply with their requirements to establish and maintain a reporting mechanism for victims. It is essential that State Attorney Generals have the authority to use their expansive resources to act against entities when their most vulnerable citizens are harmed.

5) **Appears to align with federal law.** Section 230(c)(1) of the federal Communications Decency Act of 1996 shields online platforms from liability for third-party content: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[10] This provision has been hailed as the law that created the modern internet, fostering free expression online and allowing an array of innovative services and spaces to flourish, from search engines to social media.[11] It has also come with a destructive side, absolving platforms of responsibility for virtually all third-party harms arising from the use of their services – "a protection not available to print material or television broadcasts."[12]

Section 230 was intended to promote investment in online companies and encourage "'Good Samaritan' blocking and screening of offensive material" [13] without fear of liability for defamation.[14] Courts soon adopted an expansive interpretation – a key early decision construed "publisher" immunity as encompassing "traditional editorial functions" such as deciding whether to publish, remove, or even alter content.[15] Consequently, the plaintiff, a victim of online

---

[10] 42 U.S.C. § 230(c)(1). Section 230 also (1) provides a safe harbor for good faith content moderation, (2) preempts contrary state laws, and (3) enumerates exemptions for enforcement of federal criminal statutes, intellectual property laws, communications privacy laws, and sex trafficking.
[11] See e.g., Kosseff, *The Twenty-Six Words that Created the Internet* (2019).
[12] Quinta Jurecic, "The politics of Section 230 reform: Learning from FOSTA's mistakes" *Brookings* (Mar. 1, 2022), https://www.brookings.edu/articles/the-politics-of-section-230-reform-learning-from-fostas-mistakes.
[13] § 230(c).
[14] *Fair Hous. Council v. Roommates.com, LLC* (9th Cir. 2008) 521 F.3d 1157, 1163.
[15] *Zeran v. Am. Online, Inc* (4th Cir. 1997) 129 F.3d 327.

defamation by an anonymous user, had no recourse against the platform despite its failure to timely remove the content, which would have resulted in liability in the offline world. Following this logic, courts have extended Section 230 well beyond the defamation context, routinely concluding that online intermediaries are not liable for harms related to third-party illicit content.[16] "The common thread weaving through these cases is that the courts have sapped §230's Good Samaritan concept of its meaning."[17]

This sweeping grant of immunity has been the subject of widespread criticism and calls for reform.[18] Senators Lindsey Graham and Dick Durbin are planning to introduce a bill that would sunset Section 230.[19] Justice Clarence Thomas has called for the Supreme Court to review the scope of Section 230.[20] Ninth Circuit Judge Ryan Nelson recently stated that courts have "stretch[ed] the statute's plain meaning beyond recognition," leading to "perverse effects."[21] The Ninth Circuit "should revisit our precedent," he urged, particularly in light of "artificial intelligence raising the specter of lawless and limitless protections."[22]

Section 230 has been amended once since it was adopted, following on the heels of the Backpage.com scandals. Using Section 230, Backpage was able to shield itself from several lawsuits brought by young sex trafficking victims.[23] Backpage wasn't simply a passive conduit for the sexual exploitation of minors; it helped traffickers avoid restrictions on sex ads with minors. A Senate investigation revealed that "Backpage regularly edited ads to remove keywords that would identify them as objectionable or illegal, rather than removing them outright—so ads with words like 'teenage,' 'rape,' and 'little girl,' would still be published, just with those words removed."[24] This led Congress to adopt an exemption to Section 230 for knowing facilitation of sex trafficking.[25]

AB 1394 was specifically amended in the Senate Judiciary Committee to track this exemption. This bill maintains those provisions and appears to continue to be compatible with Section 230.

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

> Given a full year to comply with California's landmark AB 1394 (Wicks and Flora) and notwithstanding soaring profits, social media platforms have apparently done nothing or next

---

[16] Michael Rustad & Thomas Koenig, "The Case for a CDA Section 230 Notice-and-Takedown Duty" (2023) 23 Nev.L.J. 533, 561-574.
[17] Danielle Keats Citron, "How to Fix Section 230" (2023) 103 B.U.L. Rev. 713, 727.
[18] E.g., John Lucas, "AG Moody Joins with Other Attorneys General to Urge Congress to Stop Protecting Illegal Activity on the Net," *Capitolist* (May 23, 2019), https://thecapitolist.com/ag-moody-joins-with-other-attorneys-general-to-urge-congress-to-stop-protecting-illegal-activity-on-the-net.
[19] Lauren Feiner, "Lawmakers are tyring to repeal section 230 again" *The Verge* (Mar. 21, 2025), https://www.msn.com/en-us/politics/government/lawmakers-are-trying-to-repeal-section-230-again/ar-AA1BptAI?ocid=BingNewsVerp.
[20] *Doe ex rel. Roe v. Snap, Inc.* (2024) 144 S. Ct. 2493 (Thomas, J., dissenting from denial of certiorari).
[21] *Calise v. Meta Platforms, Inc.* (9th Cir. 2024) 103 F.4th 732, 747 (Nelson, J. concurring) (*Calise*).
[22] *Ibid.*
[23] See e.g. *M.A. v. Vill. Voice Media Holdings* (E.D.Mo. 2011) 809 F.Supp.2d 1041.
[24] Quinta Jurecic, "The politics of Section 230 reform: Learning from FOSTA's mistakes (Mar. 1, 2022) *Brookings*, https://www.brookings.edu/articles/the-politics-of-section-230-reform-learning-from-fostas-mistakes/.
[25] Stop Enabling Sex Traffickers Act and the Allow States to Fight Online Sex Trafficking Act (SESTA/FOSTA) legislation package. (See P.L. 115-164, 113 Stat. 1253.)

to nothing to comply with that law, one compassionately aimed at protecting sexually brutalized and exploited children.

AB 1394 was prompted by the well-documented role social media platforms play in helpfully and indispensably ensuring (i) that images and videos of child rape and sex abuse (CSAM) randomly uploaded by third-party criminals are efficiently delivered to eager pedophiles even when they don't search for it and (ii) that criminal sex traffickers who profit from child rape are efficiently and inexpensively matched with pedophile customers.

Also, since AB 1394's enactment, the astonishing growth in the power and sophistication of AI means all this will soon get worse, fast. For these reasons, AB 1137 surgically makes current law stronger in the hope the platforms will do more to prevent child sex abuse and trafficking.

The National Center on Sexual Exploitation, co-sponsors of the bill, write:

This legislation represents a critical step in preventing the further spread of CSAM and protecting children from sexual exploitation online. The harms of CSAM cannot be overstated. Survivors suffer long-lasting trauma, and every time an image is shared, it compounds that harm—creating a perpetual cycle of revictimization. Online platforms, as primary vehicles for sharing this material, have a responsibility to act swiftly and decisively to remove it and assist in the identification of perpetrators.

Research supports the need for vigilance and proactive measures. The Butner Study, a landmark longitudinal study conducted by the Federal Bureau of Prisons, found that **over 85% of men convicted of offenses involving CSAM had also committed contact sexual offenses against children**, even if they had not been previously charged. This finding dismantles the myth that CSAM offenders are not hands-on offenders, and highlights the very real risk they pose to children offline as well. Additionally, the **National Center for Missing and Exploited Children (NCMEC)** received over 36 million reports to its CyberTipline in 2023 alone—many involving material circulating on mainstream platforms. These numbers demonstrate the scale of the problem and the urgent need for platforms to implement effective, human-reviewed reporting mechanisms. (Emphasis in original.)

ARGUMENTS IN OPPOSITION: In opposition to the bill, TechNet, California Chamber of Commerce, and Communications Industry Association jointly write:

Audit Frequency Is Excessive and Unjustified, and Publication of Audit Results Could Undermine Safety
Requiring twice-yearly independent audits places an extreme burden on providers, especially given the serious compliance incentives already in place through enforcement risk. The requirement is disproportionate to any demonstrated need and far exceeds norms in comparable regulatory contexts.

Furthermore, there is genuine concern about the availability of properly qualified third-party auditors for this type of specialized content moderation review. Rushing to impose rigid audit requirements without ensuring adequate capacity will result in inconsistent quality and unnecessary expense.

Publishing audit outcomes does not materially improve compliance or enforcement and would undermine such efforts. Requiring audits to be publicly disclosed could inadvertently aid malicious actors, including those seeking to exploit platform systems to distribute CSAM. Companies constantly redesign and engineer their systems to prevent sophisticated, bad actors from abusing their users and platforms. These bad actors use publicly available information to help identify weak points in systems as well as understand how platforms are deploying resources and targeting enforcement of their policies. An increase in publicly available information about these systems will unintentionally give these actors a boost in their efforts. We strongly object to the bill's requirement making these audits public. The existing transparency reporting requirements can serve enforcement and public accountability without compromising the integrity of internal safeguards.

Enforcement Focus Should Be Proportional
We support Attorney General enforcement and agree that it is a more appropriate mechanism than a private right of action. However, enforcement should target intentional or material noncompliance, with penalties scaled according to the severity of the violation. A balanced approach would protect users without overburdening responsible providers.

Premature and Unclear Justification
AB 1137 proposes significant changes to a law that only went into effect on January 1, 2025. With no demonstrated enforcement history or evidence of widespread noncompliance, it is unclear what specific problem this bill is intended to solve.

Our members are deeply committed to protecting children online. Every day, they work to strengthen systems and processes that detect and remove child sexual abuse material (CSAM). Considering that the existing statute only took effect on January 1 of this year, we believe it's too soon to conclude what is or isn't working. Rather than rushing to amend it, we would welcome an open conversation about early implementation challenges and how we can collaborate to strengthen what's already in place. We all share the same goal—keeping children safe—and we believe thoughtful, data-driven policymaking is the best path forward.

REGISTERED SUPPORT / OPPOSITION:

Support

3strands Global Foundation (Co-Sponsor)
Childrens Advocacy Institute (Co-Sponsor)
California Initiative for Technology & Democracy, a Project of California Common CAUSE
Jewish Family and Children's Services of San Francisco, the Peninsula, Marin and Sonoma Counties
National Center for Missing & Exploited Children
National Center on Sexual Exploitation (NCOSE)

Opposition

California Chamber of Commerce
Computer & Communications Industry Association
Technet-technology Network

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