Date of Hearing: April 29, 2025

ASSEMBLY COMMITTEE ON JUDICIARY
Ash Kalra, Chair
AB 1137 (Krell) – As Amended April 21, 2025

SUBJECT: REPORTING MECHANISM: CHILD SEXUAL ABUSE MATERIAL

KEY ISSUE: SHOULD THE LEGISLATURE ENHANCE CALIFORNIA'S STATUTORY FRAMEWORK FOR COMBATING ONLINE CHILD SEXUAL ABUSE MATERIAL (CSAM) AND COMMERCIAL SEXUAL EXPLOITATION BY CLOSING GAPS IN A RECENTLY ENACTED LAW?

SYNOPSIS

In 2023, the Legislature enacted AB 1394 (Wicks, Chap. 579, Stats. 2023), establishing a first-in-the-nation statutory framework to require social media platforms to remove child sexual abuse material (CSAM) reported by victims and to impose civil liability on platforms that knowingly facilitated the commercial sexual exploitation of minors through harmful design choices. That law became operative on January 1, 2025.

AB 1137 strengthens and clarifies existing provisions by (1) allowing any user—not just the depicted minor—to report CSAM; (2) requiring human review when automated systems fail to detect reported content; (3) enabling public enforcement when a reporting mechanism is inaccessible or nonfunctional; and (4) ensuring that platforms claiming a liability safe harbor have conducted independent, third-party audits that are made public. 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. This measure passed out of the Assembly Committee on Privacy and Consumer Protection by a 13-0 vote.

SUMMARY: Strengthens enforcement and accountability under California's child sexual abuse material (CSAM) reporting law by expanding who may report, requiring human review of flagged content, enabling public enforcement, and mandating independent audits of platform features that contribute to commercial sexual exploitation. Specifically, **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 the 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. Section 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. Section 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. (Penal Code Section 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. (Business and Professions Code Section 17601.)

c) "Social media company" as a person or entity that owns or operates one or more social media platforms. (Business and Professions Code Section 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. (Business and Professions Code Section 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. (Civil Code Section 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. (Civil Code Section 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, and features to detect 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. (Civil Code Section 3345.1 (g).)

FISCAL EFFECT: As currently in print this bill is keyed fiscal.

COMMENTS: Social media platforms continue to serve as central vectors for the dissemination of child sexual abuse material (CSAM) and the facilitation of commercial sexual exploitation, often through design choices that amplify harmful content or allow it to persist despite user reports. In 2023, the Legislature enacted AB 1394 (Wicks, Chap. 579, Stats. 2023) to create a statutory right for victims to demand the removal of CSAM in which they are depicted and to hold platforms liable when their systems knowingly facilitate child exploitation.

AB 1137 strengthens the law by refining and enforcing AB 1394's core protections: it expands who may report CSAM, requires human review when hash-matching fails, authorizes public

prosecutors to enforce reporting obligations, and mandates that liability-shielding audits be conducted by independent experts and made public. These measured amendments ensure that the original intent of AB 1394—protecting children from enduring digital abuse—is realized in practice. The author explains the impetus for this measure:

> 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.

Legislative history – AB 1394 (Wicks, Chap. 579, Stats. 2023). AB 1394 established California's first statutory framework to combat the proliferation of child sexual abuse material (CSAM) on social media platforms. AB 1394 was enacted in response to escalating evidence that major platforms—including Facebook, Instagram, TikTok, and others—not only host vast amounts of CSAM, but through design features such as algorithmic recommendations, livestream gifting, and unmoderated chat functions, actively facilitate its production and dissemination. As enacted, AB 1394 imposed two primary obligations:

- 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 make reasonable efforts to prevent recirculation of the same content.

- Liability for Facilitating Commercial Sexual Exploitation: The bill amended Civil Code Section 3345.1 to impose strict 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 and mitigated foreseeable risks.

AB 1394's passage followed extensive findings of fact. The bill cited whistleblower testimony revealing that Meta (Facebook and Instagram) deprioritized CSAM enforcement due to "return on investment" concerns, failed to train moderators, and permitted encrypted systems and groups to operate as hubs for trafficking. It also relied on investigative reporting showing how TikTok's livestream functions were monetizing sexualized interactions with minors. AB 1394 passed both houses of the Legislature unanimously, with votes of 77-0 on the Assembly floor and 40-0 in the Senate. It was widely supported by survivor advocates, child safety organizations, and public interest groups, and was signed into law by Governor Newsom on October 8, 2023. The law became operative on January 1, 2025.

AB 1137 builds upon this statutory foundation by refining enforcement mechanisms, expanding standing, and addressing gaps in audit transparency and reporting accessibility that have emerged in the initial months following AB 1394's implementation.

The legislative gap left by AB 1394. Social media platforms remain vectors for the viral spread of child sexual abuse material (CSAM), and existing statutory protections enacted by AB 1394—though groundbreaking—reveal gaps in existing law.

First, survivors cannot access the protections of AB 1394 unless they themselves submit the report, even when the CSAM is identified and reported by a trusted adult, clinician, teacher, or nonprofit. This limitation has created a substantial barrier for the most vulnerable users—especially traumatized minors, or those who may be unaware that such images are circulating. AB 1137 addresses this flaw by expanding reporting eligibility to any user and preserving standing for the depicted individual, thereby ensuring that victims are not barred from relief due to procedural technicalities.

Second, platforms are under no legal obligation to meaningfully review a report, unless there is a hash match, even when CSAM is obvious to a human reviewer. Hash matching tools work "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." (*NCMEC: Take It Down*, available at https://takeitdown.ncmec.org/.) 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. But as generative AI tools rapidly advance, bad actors now digitally manipulate content to avoid detection by hash-matching systems, which automated technological tools that identify known digital content—such as CSAM—by comparing the cryptographic "hash" of a file against a database of hashes corresponding to previously identified illegal material. In the absence of a human review mandate, such images may continue circulating indefinitely. AB 1137 fills this enforcement gap by requiring natural person review of reported material that does not trigger a known hash match and remains unblocked.

Third, AB 1394 lacks a clear and enforceable mechanism to ensure that the CSAM reporting portal is actually functional. Investigations by child safety advocates have documented that many major platforms bury their reporting tools deep within app settings, fragment the process across multiple interfaces, or provide pathways that lead to dead ends. Platforms can claim to have "implemented" the required reporting system while making it nearly impossible to find or use. AB 1137 resolves this deficiency by requiring a "clear and conspicuous" reporting mechanism.

Fourth, while the California Attorney General generally retains the authority to enforce any civil statute, unless expressly excluded, AB 1394 was silent on public enforcement. As a result, it was unclear whether local prosecutors or the Attorney General could enforce its provisions independently of private litigants. AB 1137 makes this enforcement power explicit. It grants the Attorney General, district attorneys, city attorneys, and county counsel clear authority to pursue civil penalties and injunctive relief for failure to maintain a functional reporting system. This amendment ensures that public enforcement does not depend on the availability of private litigants and creates a more proactive compliance framework.

Finally, the audit safe harbor provision under AB 1394 allows platforms to avoid liability for facilitating commercial sexual exploitation if they conduct biannual audits and mitigate foreseeable risks—but the law does not require those audits to be performed by independent experts or to made public. As a result, companies may self-certify compliance without scrutiny. AB 1137 attempts to correct this by requiring independent, third-party audits conducted by experts in trust and safety, and mandates public disclosure of the audit (with redaction of trade secrets).

Concerns. Industry groups argue that AB 1137 makes significant changes to AB 1394, which only became operative on January 1, 2025. They contend that enforcement data is not yet available and that the Legislature should wait before amending the law. AB 1137, however, does not revise the core obligations enacted by AB 1394—it clarifies, enforces, and according to the author, closes known loopholes identified during the implementation ramp-up period.

The majority of the concerns raised by the opposition—and the gist of the discussion in the Committee on Privacy and Consumer Protection's hearing on this bill, centered on the audit frequency and publication requirements—issues largely outside this Committee's jurisdiction. Industry representatives argue that the requirement to make CSAM-related audits public—subject to trade secret redactions—could inadvertently assist bad actors by revealing system vulnerabilities and enforcement strategies. They further argue that requiring twice-yearly independent audits places an extreme burden on providers. The audit requirement under Civil Code Section 3345.1 already existed under AB 1394, but it permitted self-directed reviews and internal disclosures. AB 1137 amends that provision to require that the audits are conducted by qualified, independent third parties and are transparent to the public, subject to redactions to protect proprietary technology.

Opponents further contend that the daily penalty for nonfunctional reporting systems is disproportionate and punitive, particularly for platforms that are making good-faith efforts to comply, and that the enforcement should be "proportional." As drafted, the daily penalty applies only when the reporting mechanism is unavailable, inaccessible, or noncompliant with statutory requirements. These failures are not minor technical glitches—they represent the entire mechanism by which survivors report CSAM and seek protection. The penalty is calibrated to ensure rapid remediation of platform failures. Moreover, AB 1137 preserves judicial discretion in the event of enforcement. Specifically, the statute permits a civil penalty of up to $250,000 per day for failure to maintain a functional reporting mechanism, but leaves the amount of the penalty to the discretion of the court, which may consider the nature of the violation, efforts to comply, and mitigating circumstances. Courts are fully empowered to impose lower penalties where appropriate, ensuring that enforcement is proportional and tailored to the facts of each case. This flexible structure ensures that serious violations can be meaningfully deterred without creating rigid or unfair burdens for platforms acting in good faith.

***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 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 Computer & Communications Industry Association jointly write:

> <u>Audit Frequency Is Excessive and Unjustified, and Publication of Audit Results Could Undermine Safety</u>
> 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 Catholic Conference
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: Shiran Zohar / JUD. / (916) 319-2334