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

SB 1217 (Grove)
Version: March 24, 2026
Hearing Date: April 13, 2026
Fiscal: Yes
Urgency: No
CK

SUBJECT

Nonconsensual Intimate Image Clearinghouse

DIGEST

This bill seeks to create a nonconsensual intimate image clearinghouse that allows victims to send such images to the California Department of Justice (DOJ) for them to verify and create "identifiers" that will then be sent to "covered platforms" who are required to take down any matching images within their systems.

EXECUTIVE SUMMARY

Over the past decade, California has enacted a series of reforms to address image-based sexual abuse, including nonconsensual pornography, child sexual exploitation, and digitally altered deepfake content. Despite these efforts, major gaps remain in the current legal framework. Victims of nonconsensual sexual content, including child sexual abuse material (CSAM), often face daunting, opaque, or ineffective takedown procedures, while the platforms profiting from that content typically avoid accountability, citing user anonymity or lack of notice.

At the federal level, the recently enacted Take It Down Act requires covered platforms to remove such content within 48 hours of notice. However, the author and sponsor argue that navigating the process with each platform where such images may appear is a daunting prospect, especially for traumatized victims.

This bill enlists DOJ to create a portal for victims to send their nonconsensual intimate images for DOJ, after verification, to create identifiers, which may include cryptographic hashes or digital fingerprints. These identifiers are then sent to "covered platforms," who must search their systems for matching identifiers and take down such images within 48 hours. The bill is sponsored by California Survivor Coalition. It is supported by numerous advocacy groups and governmental entities, including Crime Victims United and the Fresno County District Attorney. No timely opposition has been

received. Should the bill pass out of this Committee, it will next be heard by the Senate Public Safety Committee.

PROPOSED CHANGES TO THE LAW

Existing federal law:

1) Establishes the Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks (TAKE IT DOWN) Act, which defines the following relevant terms:
    a) "Consent" means an affirmative, conscious, and voluntary authorization made by an individual free from force, fraud, duress, misrepresentation, or coercion.
    b) "Digital forgery" means any intimate digital depiction of an identifiable individual created through the use of software, machine learning, artificial intelligence, or any other computer-generated or technological means, or altering an authentic visual depiction, that, when viewed as a whole by a reasonable person, is indistinguishable from an authentic visual depiction of the individual.
    c) "Identifiable individual" means an individual who appears in whole or in part in an intimate visual depiction, and whose face, likeness, or other distinguishing characteristic (including a unique birthmark or other recognizable feature) is displayed in connection with such intimate visual depiction. (47 U.S.C. § 223(h)(1).)

2) Makes it a crime for any person, in interstate or foreign commerce, to use an interactive computer service to knowingly publish an intimate visual depiction of an identifiable individual, including a digital forgery, as follows:
    a) If the person is not a minor, when the intimate visual depiction was obtained or created under circumstances in which the person knew or reasonably should have known that the identifiable individual had a reasonable expectation of privacy, the content depicted was not voluntarily exposed by the individual, the content depicted is not a matter of public concern, and the publication of the intimate visual depiction is intended to cause harm to the identifiable individual.
    b) If the person is a minor, when the depiction is posted with the intent to abuse, humiliate, harass, or degrade the minor, or to arouse or gratify the sexual desire of any person. (47 U.S.C. § 223(h)(2) & (3).)

3) Requires, not later than May 19, 2026, a covered platform to establish a process whereby an identifiable individual, or an authorized person acting on their behalf, may notify the platform of an intimate visual depiction on the platform and request its removal, with information sufficient for the platform to identify the individual and to locate the intimate visual depiction in question.

a) The platform must provide a clear and conspicuous notice of the removal process that is easy to read, in plain language, and provide information regarding the platform's obligations, including how to submit a removal notice.
b) Upon receiving a valid removal request, a covered platform shall, as soon as possible, but not later than 48 hours after receiving the request, remove the intimate visual depiction and make reasonable efforts to identify and remove any known identical copies of such depiction.
c) A platform's failure to remove an intimate visual depiction after receiving a valid request is treated as a violation of specified federal laws and may be enforced by the Federal Trade Commission. (47 U.S.C. 223a note.)

Existing state law:

1) Provides that a depicted individual has a cause of action against a person who does either of the following:
    a) Creates and intentionally discloses sexually explicit material and the person knows or reasonably should have known the depicted individual in that material did not consent to its creation or disclosure.
    b) Intentionally discloses sexually explicit material that the person did not create, and the person knows the depicted individual in that material did not consent to the creation of the sexually explicit material. (Civ. Code § 1708.86(b).)

2) Creates a private right of action against a person who intentionally distributes a photograph or recorded image of another that exposes that person's intimate body parts, as defined, or shows the other person engaged in specified sexual acts, without that person's consent, knowing that the other person had a reasonable expectation that the material would remain private, if specified conditions are met. (Civ. Code § 1708.85(a)-(c).)

3) Requires a social platform, as defined, to provide a mechanism for a user in California to report to the platform material that the user reasonably believes is CSAM depicting an identifiable minor and to permanently block such reported material when there is a reasonable basis to believe that the reported material is CSAM; failure to comply with these requirements subjects a platform to liability in a civil action for actual damage and statutory damages, as specified. (Civ. Code, §§ 3273.66, 3273.67.)

4) Criminalizes the following:
    a) Intentionally distributing or causing to be distributed the image of the intimate body part or parts of another identifiable person, or an image of the person depicted engaged in specified sexual acts when the person distributing the image knows or should know that the distribution of the

image will cause serious emotional distress, and the person depicted suffers that distress and additional circumstances are established, such as there was an agreement to keep the material private, it was knowingly recorded without the authorization of the person depicted in a private space, or it was exfiltrated from the person depicted.

b) Intentionally creating and distributing, or causing to be created or distributed, any photorealistic image, computer-generated image, or pictorial representation of an intimate body part or parts of another identifiable person, or image of them engaged in specified sexual acts, when the image was created in a manner that would cause a reasonable person to believe the image is an authentic image of the person depicted, under circumstances in which the person distributing the image knows or should know that distribution of the image will cause serious emotional distress, and the person depicted suffers that distress. (Pen. Code § 647(j)(4).)

This bill:

1) Requires DOJ to establish and maintain the Nonconsensual Intimate Image Clearinghouse to allow individuals who were exploited in California to submit a request for the removal of nonconsensual intimate images from covered platforms.

2) Requires DOJ, in connection with the above, to do all of the following:
   a) Maintain a secure internet portal to receive requests for the removal of nonconsensual intimate images. The request shall be secured using hashing or other data security techniques. DOJ may temporarily possess submitted information for the purpose of verification and identifier generation. The department shall not host, possess, or store nonconsensual intimate image content for any other purpose. The portal shall provide information on the verification and removal process and the status of a previous request.
   b) Verify the identity of the requesting individual.
   c) Verify that the images are nonconsensual intimate images.
   d) Transmit verified identifiers of images and associated metadata to covered platforms. The department may work with nonprofit entities for these purposes.
   e) Maintain a secure database of verified identifiers associated with verified nonconsensual images, but not the images.
   f) Maintain strict privacy and data security.

3) Requires a covered platform to do all of the following:
   a) Accept verified notifications from DOJ and in the manner determined by the department.

   b) Search for matching identifiers of images within their systems.
   c) Remove verified matches within 48 hours of receipt.
   d) Prevent images with identical identifiers from being uploaded after removal.

4) Provides that a covered platform that receives a verified identifier from DOJ pursuant hereto has received formal notice that the associated imagery has been verified as nonconsensual. A covered platform that acts to remove content in good faith reliance on verification made by the department is not otherwise liable.

5) Subjects small covered platforms in violation to a civil penalty of $2,500 per violation, or, if intentional, $7,500 per violation.

6) Subjects a large covered platform in violation to a civil penalty of up to $50,000 per violation, or, if malicious or knowing, up to $250,000 per violation.

7) Provides DOJ enforcement authority and clarifies that the bill does not create a private right of action. Each failure to remove a verified nonconsensual intimate image constitutes a separate violation of this section.

8) Provides that DOJ's verification process and any records therefrom, including verified identifiers generated by the clearinghouse, may be used in a proceeding, subject to the Evidence Code and local rules.

9) Requires a peace officer investigating a violation of Penal Code Section 647(j)(4) to inform the victim that they can report the presence of nonconsensual intimate images found on the internet to DOJ pursuant hereto. The officer must inform DOJ if they are able to verify the violation involves nonconsensual intimate images.

10) Defines the relevant terms, including:
   a) "Covered platform" means an online service that makes content publicly available.
   b) "Identifier" means a method capable of uniquely identifying a nonconsensual intimate image and preventing its reupload and may include, but is not limited to, cryptographic hash values, perceptual hashes, or other digital fingerprinting methods.
   c) "Nonconsensual intimate image" includes all of the following:
      i. An authentic intimate image distributed without consent, including when an image is connected to human trafficking, fraud, sexual exploitation, or coercive production practices.

ii. An image digitally altered or generated by artificial intelligence realistically depicting a person nude or engaged in sexual conduct without consent.
iii. An image created when the depicted person was a minor, if the individual is now an adult.

11) Becomes operative on January 1, 2029.

COMMENTS

1. The internet is full of CSAM, nonconsensual sexual images, and deepfake porn

CSAM was a problem before the advent of the internet, but the internet has led to a "dramatic increase" in CSAM, along with "the degree of violence and sadistic content depicted in CSAM."[1] "CSAM is readily available through virtually every internet technology, including social networking platforms, file-sharing sites, gaming devices, and mobile apps."[2] A significant amount of CSAM is exchanged through end-to-end encrypted technologies or on Dark Web sites like those on the Tor network.[3] In other cases, however, CSAM is available on supposedly legitimate pornography sites. After Nicholas Kristoff reported that Pornhub was hosting videos depicting minor sex trafficking victims,[4] Pornhub removed all of the content from the site that was uploaded by unverified community members—over 10 million of the 13.5 million videos on the site.[5]

The internet is also rife with nonconsensual sexual images of adults. Sometimes these images are of ex-partners, taken consensually at the time, but uploaded without consent and with the express purpose of getting revenge; for example, the "Is Anyone Up" website explicitly solicited revenge porn images.[6] Some images were taken consensually but obtained and posted nonconsensually, such as in 2014 when hackers stole private, intimate photos from the iCloud accounts of celebrities, including Jennifer

---

[1] U.S. Dept. of Justice, Child Sexual Abuse Material (2023) p. 5, *available at* https://www.justice.gov/d9/2023-06/child_sexual_abuse_material_2.pdf. All links in this analysis are current as of April 7, 2026.
[2] *Id.* at p. 2.
[3] *Id.*at pp. 4-5.
[4] Kristoff, *The Children of Pornhub* (Dec. 4, 2020) New York Times, https://www.nytimes.com/2020/12/04/opinion/sunday/pornhub-rape-trafficking.html.
[5] Valinsky, *Pornhub removes a majority of its videos after investigation reveals child abuse* (Dec. 15, 2020) CNN, https://edition.cnn.com/2020/12/15/business/pornhub-videos-removed/index.html.
[6] U.S District Attorney's Office for the Central District of California, Press Release: Operator of 'Revenge Porn' Website Sentenced to 2 ½ Years in Federal Prison in Email Hacking Scheme to Obtain Nude Photos (Dec. 2, 2015) https://www.justice.gov/usao-cdca/pr/operator-revenge-porn-website-sentenced-2-years-federal-prison-email-hacking-scheme.

Lawrence and Kate Upton, and posted the photos online.[7] Other images are created and posted all without the subject's knowledge, much less consent.[8]

The availability of generative AI has made it even easier for an individual to create nonconsensual sexual images. Some of these images are made for use as pornography—such sexually explicit AI-generated images that "went viral on Twitter after jumping from 4chan and a specific Telegram group dedicated to abusive images of women."[9] Some of these images are used to threaten, harass, and blackmail the persons depicted in the images. For example, the FBI is accusing an Ohio man of creating "pornographic deepfake videos of at least 10 people he was stalking and harassing," including by threatening to "blackmail [them] using AI generated images of themselves having sex with their relatives."[10] The man's search history revealed that he had searched for ClothesOff,[11] which is one of many apps that openly offer to create AI-generated nude images from photos.

Facebook and Instagram have allowed these apps to advertise on their platforms, Google Play and Apple App stores have hosted these apps for download.[12] When a Twitter[13] user posts a photo, Grok, Elon Musk's AI chatbot, will generate an image of the user without their clothes (naked or in just their underwear) in the comments upon request by another user.[14] The AI-generated image is public and viewable to the user and any of their followers.[15]

Children and teens are also victims of "undress" apps and deepfake porn generators—story[16] after story[17] has been written[18] about students[19] in middle and high schools[20]

---

[7] Arthur, *Naked celebrity hack: security experts focus on iCloud backup theory* (Sept. 1, 2014) The Guardian, https://www.theguardian.com/technology/2014/sep/01/naked-celebrity-hack-icloud-backup-jennifer-lawrence.

[8] *E.g.*, Hounsell, *She was searching online for a receipt. She found a video of herself engaged in a sex act* (Jan. 17, 2025) CBC, https://www.cbc.ca/news/canada/nova-scotia/intimate-partner-violence-sharing-intimate-images-1.7432723.

[9] Maiberg & Cole, *AI-Generated Taylor Swift Porn Went Viral on Twitter. Here's How It Got There* (Jan. 25, 2024) 404 Media, https://www.404media.co/ai-generated-taylor-swift-porn-twitter/.

[10] Cole, *A Deepfake Nightmare: Stalker Allegedly Made Sexual AI Images of Ex-Girlfriends and Their Families* (Jun. 26, 2025) 404 Media, https://www.404media.co/deepfake-harassment-ohio-undress-clothoff-nudify-apps/.

[11] *Ibid.*

[12] Maiberg, *Instagram Advertises Nonconsensual AI Nude Apps* (Apr. 22, 2024) 404 Media, https://www.404media.co/instagram-advertises-nonconsensual-ai-nude-apps/; Maiberg, *Google Bans Face Swap App for Inviting Users to Make Deepfake Porn* (Apr. 2, 2024) 404 Media, https://www.404media.co/google-bans-face-swap-app-for-advertising-deepfakes-on-porn-sites/.

[13] Aka "X."

[14] Shalabaieva, *Elon Musk's Grok AI Will 'Remove Her Clothes" In Public, On X* (May 6, 2025) 404 Media, https://www.404media.co/elon-musks-grok-ai-will-remove-her-clothes-in-public-on-x/.

[15] *Ibid.*

[16] Koebler & Maiberg, *'What Was She Supposed to Report?:' Police Report Shows How a High School Deepfake Nightmare Unfolded* (Feb. 15, 2024) 404 Media, https://www.404media.co/what-was-she-supposed-to-report-police-report-shows-how-a-high-school-deepfake-nightmare-unfolded/.

generating[21] fake nude and/or pornographic images[22] of their fellow students[23] and sharing the images with their friends.[24] Female and LGBTQ+ students are far more likely to be depicted in deepfaked nonconsensual imagery.[25] Major AI and tech companies have also facilitated the creation of massive amounts of AI-generated CSAM.[26] AI generative technologies "are also being employed to facilitate the grooming and sextortion of minor victims."[27]

2. Regulatory response

In response to these issues, California passed AB 602 (Berman, Ch. 491, Stats. 2019), which provides a cause of action against a person who creates and intentionally discloses sexually explicit, nonconsensual deepfakes, as specified, and those who intentionally disclose them knowing they are nonconsensual. AB 621 (Bauer-Kahan, Ch. 673, Stats. 2025) updated the law to combat this troubling new trend of GenAI nudification and provided stronger enforcement mechanisms to incentivize compliance. It expanded the cause of action to include material depicting minors and extends

---

[17] Reuters, *Spanish prosecutor to probe AI-generated images of naked minors* (Sept. 25, 2023) Reuters, https://www.reuters.com/world/europe/spanish-prosecutor-probe-ai-generated-images-naked-minors-2023-09-25/.
[18] Healey, *Beverly Hills middle school rocked by AI-generated nude images of students* (Feb. 26, 2024) Los Angeles Times, https://www.latimes.com/california/story/2024-02-26/beverly-hills-middle-school-is-the-latest-to-be-rocked-by-deepfake-scandal.
[19] Ciavaglia, *Council Rock middle schooler investigated over alleged deepfake images of girls* (Jun. 6, 2025) phillyburbs.com, https://www.phillyburbs.com/story/news/local/2025/06/06/council-rock-newtown-middle-school-deepfake-ai-technology-police-investigation-porn-bucks-county/84029305007/.
[20] Blume, *L.A. school district probes inappropriate images shared at Fairfax High. More AI abuse?* (Apr. 9, 2024) Los Angeles Times, https://www.latimes.com/california/story/2024-04-09/student-generated-inappropriate-ai-image-of-girls-at-fairfax-high.
[21] Haskell, *Calabasas teen says classmate not disciplined for sharing real and fake images of her* (Mar. 14, 2024) ABC 7 Eyewitness News, https://abc7.com/calabasas-high-school-student-accuses-classmate-sharing-real-and-fake-nude-photos/14521422/.
[22] McNicholas, *New Jersey high school students accused of making AI-generated pornographic images of classmates* (Nov. 2, 2023) CBS News, https://www.cbsnews.com/newyork/news/westfield-high-school-ai-pornographic-images-students/.
[23] Fry, *Laguna Beach High School investigates 'inappropriate' AI-generated images of students* (Apr. 2, 2025) Los Angeles Times, https://www.latimes.com/california/story/2024-04-02/laguna-beach-high-school-investigating-creation-of-ai-generated-images-of-students.
[24] Guardian staff, *Sydney teenager allegedly used AI to create deepfake pornography of students* (Jan. 8, 2025) The Guardian, https://www.theguardian.com/australia-news/2025/jan/09/sydney-high-school-ai-deepfake-porn-scandal-ntwnfb.
[25] Center for Democracy & Technology, In Deep Trouble: Surfacing Tech-Powered Sexual Harassment in K-12 Schools (Sept. 2024) p. 18, *available at* https://cdt.org/insights/report-in-deep-trouble-surfacing-tech-powered-sexual-harassment-in-k-12-schools/.
[26] *E.g.*, Maiberg, *Tech Companies Promise to Try to Do Something About All the AI CSAM They're Enabling* (Apr. 29, 2024) 404 Media, https://www.404media.co/tech-companies-promise-to-try-to-do-something-about-all-the-ai-csam-theyre-enabling/.
[27] Thoel. Stroebel, & Portnoff, Generative ML and CSAM: Implications and Mitigations (Jun. 24, 2023) Thorn & Stanford Internet Observatory, p. 8.

liability to those knowingly facilitating or recklessly aiding or abetting the actionable conduct. It also took aim at "deepfake pornography services" whose primary purpose is to create these sexually explicit deepfakes.

However, once CSAM or nonconsensual intimate imagery is online, it can be virtually impossible to get it taken down. California now has laws requiring social media platforms to have reporting mechanisms for nonconsensual images and CSAM,[28] though it is unclear how responsive the platforms have been. In May 2025, Congress enacted the TAKE IT DOWN Act, which makes it illegal to knowingly publish or threaten to publish nonconsensual sexual images, and beginning in May 2026, requires a website or social media company to remove such material within 48 hours' notice from a victim.[29] The TAKE IT DOWN Act was inspired in part by a teen whose classmates posted deepfake images of her to Snapchat, which Snapchat refused to take down for nearly a year.[30]

This bill seeks to enlist California's DOJ in the effort to get these images taken down from the internet.

According to the author:

> Human trafficking survivors often endure long-lasting trauma from the persistent circulation of intimate images created through coercion, threats, deception, or manipulation. While federal law provides a framework for platforms to remove such content, victims frequently face significant barriers in navigating complex reporting processes. SB 1217 creates a secure, coordinated Nonconsensual Intimate Image Clearinghouse within the Department of Justice to verify requests, generate digital identifiers, and streamline notifications to covered platforms for timely removal. SB 1217 represents a thoughtful, victim-centered approach that complements federal efforts and empowers California to better protect survivors of exploitation and abuse.

The bill requires, starting January 1, 2029, DOJ to establish and maintain the Nonconsensual Intimate Image Clearinghouse to allow individuals who were exploited in California to submit a request for the removal of nonconsensual intimate images from covered platforms. DOJ must maintain a secure internet portal to receive requests for the removal of such images. The request shall be secured using hashing or other data security techniques.

---

[28] *See* Bus. & Prof. Code, § 22671; Civ. Code, § 3273.66.
[29] Pub. L. No. 119-12 (May 19, 2025) 139 Stat. 55.
[30] Ortutay, *President Trump signs Take It Down Act, addressing nonconsensual deepfakes. What is it?* (May 20, 2025) AP News, https://apnews.com/article/take-it-down-deepfake-trump-melania-first-amendment-741a6e525e81e5e3d8843aac20de8615.

The process envisioned by the bill has victims actually transmit the intimate images to DOJ, who at least temporarily hosts the images. Upon receiving the image, DOJ must verify the identity of the individual and that the images are, in fact, nonconsensual intimate images. Then, DOJ must create "identifiers," which may include some form of hashing or digital fingerprinting, for the images. DOJ must then send these identifiers to all "covered platforms" and maintain a database of identifiers and allow for the checking of status of a previous request.

DOJ then sends these identifiers and associated metadata to all "covered platforms." The bill authorizes DOJ to work with nonprofits for this part of the process. Covered platforms are then required to receive them and search for matching identifiers within their systems. Similar to federal law, covered platforms must remove matches within 48 hours. A covered platform that receives a verified identifier from DOJ pursuant hereto has received formal notice that the associated imagery has been verified as nonconsensual.

The bill provides for civil penalties against platforms in violation based on size and whether the violation was intentional or malicious and knowing.

3. Concerns with the Clearinghouse and process

While enlisting a powerful ally for victims to take down such images online is a compelling goal, some concerns have been raised about the process and potential unintended consequences. First, a process by which victims are actually transmitting these intimate images may jeopardize their privacy and provide a ripe target for perpetrators looking to exfiltrate such images. Given that DOJ must maintain the images at least long enough to verify the individual submitting them, and presumably that the individual is in the image, and that it qualifies as a "nonconsensual intimate image," heightens these privacy concerns.

For example, the National Center for Missing and Exploited Children (NCMEC) currently provides a free service that helps remove or stop the online sharing of such images of minors. The service creates a "hash" of the relevant image or video. But the image or video **remains on the reporting party's device and is not actually submitted as part of the process.** Instead, the unique hash that was created is added to NCMEC's hash list, which is then made available to online platforms who may scan their public or unencrypted services to detect, remove, and where appropriate, report those images or videos to NCMEC. NCMEC describes the technology in layman's terms: "Think of a hash value like a digital fingerprint. Each image or video gets a unique hash value that distinguishes it from other images and videos."[31]

[31] https://takeitdown.ncmec.org/faq/

In addition, it is not clear that DOJ has the technical capability to securely receive intimate images, potentially including CSAM, and create a hash or digital fingerprint. The author may wish to consider a different process for securing these identifiers.

Next, there is some concern with the breadth and clarity of some of the definitions within the bill. "Covered platform," for instance, is broadly defined to include any online service that makes content publicly available. This may very well be every single website on the internet. That would mean DOJ must send these identifiers to every website and that every website would need to check its systems to avoid liability. In addition, the definition of "nonconsensual intimate image" includes all of the following:

- An authentic intimate image distributed without consent, including when an image is connected to human trafficking, fraud, sexual exploitation, or coercive production practices.
- An image digitally altered or generated by artificial intelligence realistically depicting a person nude or engaged in sexual conduct without consent.
- An image created when the depicted person was a minor, if the individual is now an adult.

The first category indicates the image must be "intimate," but the bill does not define the term. The author may wish to include a definition to avoid capturing a much larger universe than intended. The final category only requires the image to be of a minor with no mention of consent or it needing to be intimate. Again, the author may wish to refine these definitions to more precisely target the images intended.

In response to these concerns, the author has agreed to amendments that do the following:

- Provide a definition for what an "intimate image" is.
- Remove application to images of minors.
- Refine the definition of "covered platform" to apply to online services that make user-generated content available to the public with certain exemptions.

The author has also agreed to continue to work with the Committee on the highlighted privacy and security concerns outlined above and to further refine the verification process envisioned by the bill.

4. Stakeholder positions

The California Survivor Coalition, the sponsor of this measure, writes:

> While federal law under the TAKE IT DOWN Act requires platforms to remove NCII within 48 hours of valid notice, the burden of navigating that process remains entirely on the survivor. There is currently no centralized, trauma-informed system in California to assist victims in exercising this right. Survivors are left to repeatedly locate, document, and

> report their own abuse across countless platforms; an impossible and deeply harmful expectation.
>
> SB 1217 directly addresses this gap by establishing a secure, state-administered clearinghouse within the Department of Justice. This system will allow survivors to submit verified requests for removal, after which the Department will authenticate the request, generate unique identifiers, and transmit them to covered platforms. Platforms will then be required to remove matching content within 48 hours and take reasonable steps to prevent its reupload.

Crime Victims United writes in support:

> By shifting the burden away from victims and creating a coordinated enforcement mechanism, SB 1217 addresses the ongoing harm caused by the widespread distribution of exploitative images, including harassment, blackmail, and long-term emotional and economic damage. This measure strengthens accountability for online platforms while providing victims with meaningful tools to reclaim their safety and privacy.

SUPPORT

California Survivor Coalition (sponsor)
3strands Global Foundation
California Massage Therapy Council
Central Valley Justice Coalition
Chino Police Department
Church Without Walls
City of Mcfarland
Community Action Partnership of Kern
County of Tulare
Crime Victims United
Empowerment (Dess Perkins Foundation)
Farmersville Police Department
Fresno County Board of Supervisors
Fresno County District Attorneys Office
Fresno Police and Fire Chaplaincy
Fresno Police Department
Kern Coalition Against Human Trafficking
Kern County Sheriff's Office
Riverside County Sheriff's Office
San Luis Obispo County District Attorney
Table Mountain Rancheria
The California Baptist Capitol Ministry

Treasures
Tulare County Child Abuse Prevention Council
4 Individuals

OPPOSITION

None received

RELATED LEGISLATION

AB 392 (Dixon, 2025) requires the operator of a pornographic internet website, as defined, to obtain from its users a verification that sexually explicit material the user is uploading to the site does not include a depiction of a person who was a minor at the time the material was created, a person who did not consent to be in the material, or who did not consent to have the material uploaded, and establishes a rebuttable presumption that the failure to do so violates the operator's duty of care, as specified. AB 392 was held in the Senate Appropriations Committee.

SB 981 (Wahab, Ch. 292, Stats. 2024) required social media platforms to provide a mechanism for reporting "sexually explicit digital identity theft," essentially the posting of nonconsensual, sexual deepfakes; and requires platforms to timely respond and investigate and to remove instances of this material, as provided.

AB 1394 (Wick, Ch. 579, Stats. 2023) required social media platforms to provide a reporting mechanism for suspected child sexual abuse material and requires them to permanently block the material, as provided. It also prohibited platforms from knowingly facilitating, aiding, or abetting minor's commercial sexual exploitation.

AB 602 (Berman, Ch. 491, Stats. 2019) See Executive Summary and Comment 2.

****