

Date of Hearing: March 18, 2025

Fiscal: Yes

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION

Rebecca Bauer-Kahan, Chair

AB 621 (Bauer-Kahan) – As Introduced February 13, 2025

PROPOSED AMENDMENTS

SUBJECT: Deepfake pornography

SYNOPSIS

AB 602 (Berman; Ch. 491, Stats. 2019) created a cause of action for individuals depicted in nonconsensual deepfake pornography against those who intentionally create or distribute it. The bill was sponsored by SAG-AFTRA, and was prompted in part by the growing problem of deepfakes of celebrities. At the time, creating deepfake pornography required significant technological sophistication.

The advent of generative artificial intelligence (GenAI) has democratized this form of sexual abuse. Consumer-facing “nudification” websites and mobile applications enable the use of a person’s likeness to create highly-realistic pornographic imagery and videos with a click of a button – all without the depicted person’s consent. These images and videos can go viral among the person’s friends, family, employer, community, and beyond. Collectively, these sites have amassed hundreds of millions of visits. The impact on victims – almost always women and girls – is devastating.

In August of 2024, San Francisco City Attorney David Chiu filed a lawsuit against 16 “nudification” websites under his general enforcement authority pursuant to California's Unfair Competition Law, alleging that nudification websites violate California law, including AB 602.

This bill, sponsored by City Attorney Chiu, augments the enforcement tools available to public prosecutors and harmed individuals by updating AB 602 in several key respects. First, the bill expressly provides that the cause of action under AB 602 applies to nudification websites. In doing so, the bill is intended to be declarative of existing law, which implicitly applies to these sites. Second, the bill strengthens the existing authority of public prosecutors to hold operators of these websites accountable. Third, the bill expands the statute to apply to enablers of those who create and distribute these images, including entities that provide services to nudification websites. Finally, the bill makes a handful of additional clarifying and conforming changes.

The bill is supported by the California District Attorneys Association and Consumer Attorneys of California. It is opposed by California Civil Liberties Advocacy, which raises concerns relating to free speech, platform liability, and enforcement scope. Amendments are set forth in Comment 6.

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

THIS BILL:

- 1) Recasts and expands Civil Code section 1708.86 – the statute grants a civil cause of action against creators and distributors of deepfake nonconsensual sexually explicit material – in several ways, including by:
 - a. Revising certain definitions, including recasting:
 - i. “Sexually explicit material” as “digitized sexually explicit material,” which is defined as any portion of a visual or audiovisual work created or substantially altered through digitization that shows the depicted individual in the nude or appearing to engage in or be subject to, sexual conduct.
 - ii. “Depicted individual” as an individual who is portrayed in sexually explicit material as a result of digitization.
 - b. Clarifying that a cause of action by or on behalf of a depicted individual is not limited to circumstances in which the individual is depicted as giving a “performance.”
 - c. Providing that a minor cannot consent to creation and distribution of digitized sexually explicit material depicting the minor.
 - d. Applying the statute to instances in which the person who discloses the digitized sexually explicit material reasonably should have known the depicted individual did not consent to its creation.
 - e. Expressly including “deepfake pornography services,” defined as an internet website, mobile application, or other service that creates digitized sexually explicit material. Such websites are deemed to engage in the creation and disclosure of digitized sexually explicit material and are presumed to know that a depicted individual did not consent to the creation or disclosure of digitized sexually explicit material if they cannot produce evidence of the depicted individual’s express written consent (provided that the individual is an adult).
 - f. Applying the statute to persons that knowingly or recklessly facilitate, aid, or abet the unlawful creation or disclosure of digitized sexually explicit material. Persons that provide services to deepfake pornography services are presumed to act with knowledge or recklessness if (1) a plaintiff provided the person with evidence demonstrating that the internet website or mobile application served by the person is a deepfake pornography service that violates the statute, and (2) the person failed to stop providing services to that entity within 30 days of receiving the evidence.
 - g. Increasing the maximum civil penalty available to depicted individuals from \$30,000 to \$50,000.
 - h. Clarifying the authority of public prosecutors to enforce its provisions by expressly granting such authority. Augmenting this authority by providing that civil prosecutors may seek a civil penalty of \$25,000 per violation or \$50,000 per violation where the act was committed with malice.

- 2) Finds and declares that the provisions of the bill that clarify that a deepfake pornography service is subject to Section 1708.86 are declaratory of existing law.

EXISTING LAW:

- 1) Under the Unfair Competition Law, grants certain public prosecutors civil enforcement authority for unlawful, unfair, or fraudulent acts or practices. (Bus. & Prof. Code § 17200 et seq.) Violations are punishable by a civil penalty of up to \$2,500. (Bus. & Prof. Code § 17206(a).)
- 2) Grants a cause of action for a depicted individual 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.
- 3) Defines, among other terms:
 - a. “Digitization” as realistically depicting any of the following:
 - i. The nude body parts of another human being as the nude body parts of the depicted individuals.
 - ii. Computer-generated nude body parts as the nude body parts of the depicted individual.
 - iii. The depicted individual engaging in sexual conduct in which the depicted individual did not engage.
 - b. “Depicted individual” as an individual who appears, as a result of digitization, to be giving a performance they did not actually perform or to be performing in an altered depiction.
 - c. “Sexually explicit material” as any portion of an audiovisual work that shows the depicted individual in the nude or appearing to engage in, or being subjected to, sexual conduct.
- 4) Provides that a prevailing plaintiff who suffers harm as a result of a violation of these provisions may recover any of the following:
 - a. An amount equal to the monetary gain made by the defendant from the creation, development, or disclosure of the sexually explicit material.
 - b. One of the following:

- i. Economic and noneconomic damages proximately caused by the disclosure of the sexually explicit material, including damages for emotional distress.
 - ii. Upon request of the plaintiff at any time before the final judgment is rendered, the plaintiff may instead recover an award of statutory damages for all unauthorized acts involved in the action, with respect to any one work, as follows:
 - iii. A sum of not less than \$1,500 but not more than \$30,000.
 - iv. If the unlawful act was committed with malice, the award of statutory damages may be increased to a maximum of \$150,000.
 - c. Punitive damages.
 - d. Reasonable attorney's fees and costs.
 - e. Any other available relief, including injunctive relief.
- 5) Provides that a defendant is not liable under either of the following circumstances:
 - a. The person discloses the sexually explicit material in the course of reporting unlawful activity, exercising the person's law enforcement duties, or hearings, trials, or other legal proceedings.
 - b. The material is a matter of legitimate public concern, a work of political or newsworthy value or similar work, or commentary, criticism, or disclosure that is otherwise protected by the California or United States Constitution.
- 6) Precludes a defendant from asserting a defense that there is a disclaimer in the sexually explicit material that communicates that the inclusion of the depicted individual in the sexually explicit material was unauthorized or that the depicted individual did not participate in the creation of the development of the material.
- 7) Contains a severability clause. (Civ. Code § 1708.86.)

COMMENTS:

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

AB 621 strengthens civil enforcement mechanisms against nudity websites that use artificial intelligence to create fake nude images of real people. These sites are most often used on photos without the consent of the individuals in them and have a detrimental impact on the victims, taking away both their autonomy and their privacy. In one recent instance, five students were expelled from a Beverly Hills Middle School after creating and sharing AI generated nude photos of their classmates. The accountability laws regarding such sites must be updated to close gaps and ensure that all those who facilitate and platform these sites are held responsible. AB 621 makes important progress towards protecting the privacy and safety of women and girls online.

2) **Artificial Intelligence.** Artificial Intelligence (AI) refers to the mimicking of human intelligence by artificial systems, such as computers.¹ AI uses algorithms – sets of rules – to transform inputs into outputs. Inputs and outputs can be anything a computer can process: numbers, text, audio, video, or movement. AI that are trained on small, specific datasets in order to make recommendations and predictions are sometimes referred to as “predictive AI.” This differentiates them from GenAI, which are trained on massive datasets in order to produce detailed text and images. When Netflix suggests a TV show to a viewer, the recommendation is produced by predictive AI that has been trained on the viewing habits of Netflix users. When DALL-E generates high-resolution, lifelike images, it uses GenAI that has been trained on roughly 250 million text-image pairs.

The creation of text, imagery, video, and audio by GenAI has the potential to change the world by automating repetitive tasks and fostering creativity. When employed by bad actors, however, these capabilities have the potential to invade privacy and disrupt the lives of Californians.

3) **Nudification websites.** Since its inception, GenAI has been used to create nonconsensual pornography, more accurately referred to by sexual assault experts as image-based sexual abuse – almost entirely against women and girls.

While high-profile celebrities were most often targeted when this technology was first developed,² open-source GenAI models have been exploited to make this technology more accessible and affordable. This has led to a proliferation of websites and phone-based apps – some of which have been promoted on app stores – that offer user-friendly interfaces for uploading clothed images of real people to generate photorealistic nude images of not only adults, but also children. According to a recent *New York Times* article:

Boys in several states have used widely available “nudification” apps to pervert real, identifiable photos of their clothed female classmates, shown attending events like school proms, into graphic, convincing-looking images of the girls with exposed A.I.-generated breasts and genitalia. In some cases, boys shared the faked images in the school lunchroom, on the school bus or through group chats on platforms like Snapchat and Instagram, according to school and police reports.³

In February 2024, deepfake nude images of 16 eighth-grade students were circulated among students at a California middle school.⁴ Similar reports of abuses, almost always against girls,

¹ AB 2885 (Bauer-Kahan; Ch. 843, Stats. 2024) defined the AI as “an engineered or machine-based system that varies in its level of autonomy and that can, for explicit or implicit objectives, infer from the input it receives how to generate outputs that can influence physical or virtual environments.”

² Brian Contreras, “Tougher AI Policies Could Protect Taylor Swift—And Everyone Else—From Deepfakes,” *Scientific American* (Feb. 8, 2024), www.scientificamerican.com/article/tougher-ai-policies-could-protect-taylor-swift-and-everyone-else-from-deepfakes/.

³ Natasha Singer, “Teen Girls Confront an Epidemic of Deepfake Nudes in Schools,” *New York Times* (Apr. 8, 2024), <https://www.nytimes.com/2024/04/08/technology/deepfake-ai-nudes-westfield-high-school.html>.

⁴ Mackenzie Tatananni, “‘Inappropriate images’ circulate at yet another California high school, as officials grapple with how to protect teens from AI porn created by classmates,” *Daily Mail* (Apr. 11, 2024), <https://www.dailymail.co.uk/news/article-13295475/Inappropriate-images-California-Fairfax-High-School-AI-deepfake.html>.

have been reported across the country and show no sign of abating.⁵ In the first six months of 2024, some of the most popular nudification websites had been visited over 200 million times.⁶ Meanwhile, a 2024 study from Center on Democracy and Technology reports that 40% of students were aware of deepfakes being shared at school, 15% of which depicted an individual in a sexually explicit or intimate manner. In over 60% of these cases, the images were distributed via social media.⁷ This provides a potent means of amplifying deepfake image-based sexual abuse material, extending the content's reach by, in effect, crowdsourcing abuse – potentially reaching thousands or even millions of viewers.

Deepfake pornography can inflict profound psychological trauma. In a recent *Guardian* article, gender equity expert and journalist Luba Kassova argues that “nonconsensual deepfake pornography has become a growing human rights crisis.” She asks readers to:

Imagine finding that someone has taken a picture of you from the internet and superimposed it on a sexually explicit image available online. Or that a video appears showing you having sex with someone you have never met.

Imagine worrying that your children, partner, parents or colleagues might see this and believe it is really you. And that your frantic attempts to take it off social media keep failing, and the fake “you” keeps reappearing and multiplying. Imagine realising that these images could remain online for ever and discovering that no laws exist to prosecute the people who created it.⁸

Writing in support of the bill, the Joyful Heart Foundation states:

Unlike in the past, when creating synthetic intimate images was a complicated process, recent AI technology has made it disturbingly easy to produce highly realistic, artificial intimate images—especially through “nudify” websites and apps that simplify the process even further. With a single click, these images can spread globally, making them almost impossible to contain, while victims have little to no means of reclaiming control over their image. Women and girls are particularly vulnerable, but boys and men can be affected too. Recently, the FBI has warned of an uptick in extortion schemes targeting boys using nonconsensual AI-generated intimate images. No one is safe from this type of attack.

⁵ Tim McNicholas, “New Jersey high school students accused of making AI-generated pornographic images of classmates,” *CBS News* (Nov. 2, 2023), <https://www.cbsnews.com/newyork/news/westfield-high-school-ai-pornographic-images-students/>; Lauraine Langreo, “Students Are Sharing Sexually Explicit ‘Deepfakes.’ Are Schools Prepared?” *Ed Week* (Sept. 26, 2024), <https://www.edweek.org/leadership/students-are-sharing-sexually-explicit-deepfakes-are-schools-prepared/2024/09>; Gabrielle Hunt and Daryl Higgins “AI nudes of Victorian students were allegedly shared online. How can schools and parents respond to deepfake porn?,” *The Guardian* (June, 12, 2024), <https://www.theguardian.com/australia-news/article/2024/jun/12/ai-nudes-of-victorian-students-were-allegedly-shared-online-how-canschools-and-parents-respond-to-deepfake-porn>.

⁶ *People of the State of California v. Sol Ecom, Inc, et al.* (2024) Case No. CGC-24-617237, p. 2, https://www.sfcityattorney.org/wp-content/uploads/2024/08/2024-08-16-First-Amended-Complaint_Redacted.pdf.

⁷ Elizabeth Laird, Maddy Dwyer and Kristin Woelfel, “In Deep Trouble: Surfacing Tech-Powered Sexual Harassment in K-12 Schools,” Center for Democracy & Technology (Sept. 26, 2024), <https://cdt.org/wp-content/uploads/2024/09/FINAL-UPDATED-CDT-2024-NCII-Polling-Slide-Deck.pdf>.

⁸ Kassova, Luba. “Tech bros need to realise deepfake porn ruins lives – and the law has to catch up,” *The Guardian* (Mar. 1, 2024), <https://www.theguardian.com/global-development/2024/mar/01/tech-bros-nonconsensual-sexual-deepfakes-videos-porn-law-taylor-swift>.

Though digitally altered images are fake, the harm is real and dehumanizing. These images are weaponized to extort, bully, threaten, and humiliate victims. Survivors of this abuse suffer real life impacts, including anxiety, depression, and physical health problems. They often have to obtain restraining orders, change jobs and residences, and endure public judgment and humiliation. Some lose their careers and social circles. Survivors have described the experience as “torture for the soul” and “hell on Earth.”

The problem has become so pervasive that the United States Department of Justice recently launched the first national 24/7 helpline for survivors of image-based sexual abuse.⁹ According to RAINN, a non-profit anti-sexual assault organization, more than 100,000 deepfake images and videos are posted on the internet every day.¹⁰ The *2023 State of Deepfakes* report found in its survey of American men that 74 percent of deepfake pornography users did not feel guilty about their consumption. According to the report’s authors, this finding suggests that deepfake pornographic content is becoming normalized and accepted. Further, of those surveyed almost one-third of those surveyed stated that they did not think that deepfake pornography hurt anyone as long as it was only used for their personal interest.¹¹

In August of 2024, San Francisco City Attorney David Chiu filed a lawsuit against 16 nudification websites.¹² The lawsuit is based on the City Attorney’s general enforcement authority pursuant to California’s Unfair Competition Law (UCL), which prohibits any “unlawful, unfair, or fraudulent business act or practice.” Among the laws the complaint alleges the nudification websites violated is Civil Code section 1708.86.¹³ Added by AB 602 (Berman, 2019), section 1708.86 grants a cause of action for an individual depicted in deepfake pornography against a person who intentionally creates or discloses the deepfake pornography without the consent of the individual.

4) What this bill would do. This bill updates section 1708.86 in several key ways, including:

Express application to nudification websites. This bill expressly provides that section 1708.86 encompasses “deepfake pornography services,” defined as an internet website, mobile application, or other service that, through digitization, creates digitized sexually explicit material. The bill states that this change is declaratory of existing law. Under the bill, such websites are deemed to be engaged in the creation and intentional disclosure of digitized sexually explicit material, and are presumed to know that a depicted individual did not consent to the creation or disclosure of digitized sexually explicit material if the website cannot produce evidence of the depicted individual’s express written consent (provided that the individual is an adult).

Express authority for public prosecutors. AB 602 did not expressly grant authority to public prosecutors (the Attorney General, city attorneys, county counsel, and district attorneys).

⁹ Travers, Karen and Emmanuelle Saliba. “Fake explicit Taylor Swift images: White House is ‘alarmed’,” *ABC News* (Jan. 26, 2024), <https://abcnews.go.com/US/white-house-calls-legislation-regulate-ai-amid-explicit/story?id=106718520>.

¹⁰ *Ibid.*

¹¹ *2023 State of Deepfakes: Realities, Threats, and Impact*, Home Security Heroes, <https://www.homesecurityheroes.com/state-of-deepfakes/#deepfake-porn-survey>.

¹² Chase DiFelicianantonio, “S.F. sues websites over explicit, nonconsensual AI-generated nude images,” *San Francisco Chronicle* (Aug. 16, 2024), <https://www.sfchronicle.com/sf/article/s-f-lawsuit-deepfake-ai-19657265.php>.

¹³ *People of the State of California v. Sol Ecom, Inc, et al.* (2024) Case No. CGC-24-617237, https://www.sfcityattorney.org/wp-content/uploads/2024/08/2024-08-16-First-Amended-Complaint_Redacted.pdf.

However, under the UCL, certain public prosecutors have broad authority to pursue civil enforcement against entities that violate California's laws. This bill expressly grants standing to all public prosecutors, thereby enabling them to seek higher civil penalties than provided under the UCL.

Augmented liability. This bill expands the maximum statutory damages available to depicted individuals from \$30,000 to \$50,000. The bill also provides that civil prosecutors may seek a civil penalty of \$25,000 per violation or \$50,000 per violation where the act was committed with malice. For comparison, under the UCL, the civil penalty available to public prosecutors is \$2,500.

Expansion to enablers of violators. Often nudification websites are operated by fly-by-night fictitious entities that are in other counties, beyond the reach of California's laws. To help ensure that their operation is not enabled by legitimate entities who provide services essential for the operation of these websites – such as payment processors – the bill provides that those who knowingly or recklessly facilitate the websites, or the creation or distribution of these deepfakes, are subject to liability as well. Persons that enable the operation of a deepfake pornography service are presumed to act with knowledge or recklessness if both of the following apply:

- A plaintiff provided the person with evidence demonstrating that the internet website or mobile application served by the person is a deepfake pornography service that violates the statute; and
- The person failed to stop providing services to that entity within 30 days of receiving the evidence.

No minor consent. AB 602 applies only to consensual pornographic deepfakes, but does not distinguish between deepfakes of adults and minors, inadvertently allowing for the possibility that a minor could consent to such deepfakes. This bill clarifies that the consent exception is inapplicable to minors.

No longer limited to “performances.” AB 602 was sponsored by SAG-AFTRA. A principal focus of the bill was on protecting celebrities depicted in sexual deepfake “performances” a term used throughout the statute. This bill makes it clear that the law's application extends beyond performances to all nonconsensual depictions of individuals.

5) Constitutional considerations. Writing in opposition, California Civil Liberties Advocacy raises concerns relating to freedom of speech and federal preemption.

First Amendment. The United States and California Constitutions prohibit abridging, among other fundamental rights, freedom of speech.¹⁴ When AB 602 and an identical bill, SB 564 (Leyva, 2019), were being considered, First Amendment scholar and professor of constitutional law Erwin Chemerinsky, concluded that the legislation did not pose “any issues of constitutional concern.” Of SB 564, he wrote:

While the content regulated by this statute may be “speech” insofar as the First Amendment is concerned, it is a longstanding precept of First Amendment doctrine that “not all speech is

¹⁴ U.S. Const., 1st and 14th Amends; Cal. Const. art. I, § 2.

of equal First Amendment importance.” *See, e.g., Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, 472 U.S. 749, 758-759 (1985). And it is likewise true that “speech on matters of purely private concern is of less First Amendment concern.” *Id.* at 759. The U.S. Supreme Court has correctly recognized that “sexual behavior” is “the most private human conduct.” *Lawrence v. Texas*, 539 U.S. 558, 567 (2003). By regulating the nonconsensual use of an individual’s persona in sexually explicit audiovisual works, Senate Bill 564 does not target any forms of expression that have historically received First Amendment protection.

AB 602, which contains exceptions for certain protected speech categories,¹⁵ has been on the books for over half a decade and does not appear to have been challenged. AB 621 does not alter the type of content that section 1708.86 applies to but rather the entities that may be subjected to the law – namely, those who knowingly facilitate the creation and disclosure of nonconsensual deepfake pornography. In this regard, nearly every state, California included, has adopted “revenge pornography” statutes that vary widely in their elements, requirements, definitions and penalties. And yet “none of these statutes have ultimately been struck down as unconstitutional.”¹⁶ Given the similarities, there does not appear to be strong basis for expecting a different outcome for this bill.

Federal preemption. 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.”¹⁷ 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.¹⁸ 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.”¹⁹

Section 230 was intended to promote investment in online companies and encourage “‘Good Samaritan’ blocking and screening of offensive material”²⁰ without fear of liability for defamation.²¹ 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.²² Consequently, the plaintiff, a victim of online defamation by an anonymous user, had no recourse against the platform despite its failure to

¹⁵ 1708.86(c)(1)(B) provides that liability does not apply if the material is a matter of legitimate public concern, a work of political or newsworthy value or similar work, or commentary, criticism, or disclosure otherwise protected by the California Constitution or United States Constitution.

¹⁶ *State v. Katz* (Ind. 2022) 179 N.E.3d 431, 450, citing, among other cases, *People v. Iniguez* (2016) 247 Cal. App. 4th Supp. 1 (upholding California’s revenge pornography law).

¹⁷ 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.

¹⁸ *See e.g., Kosseff, The Twenty-Six Words that Created the Internet* (2019).

¹⁹ 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>.

²⁰ § 230(c).

²¹ *Fair Hous. Council v. Roommates.com, LLC* (9th Cir. 2008) 521 F.3d 1157, 1163 (*Roommates.com*), discussing *Stratton Oakmont, supra*, 1995 N.Y. Misc. LEXIS 229.

²² *Zeran v. Am. Online, Inc* (4th Cir. 1997) 129 F.3d 327.

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, including nonconsensual intimate images.²³ “The common thread weaving through these cases is that the courts have sapped §230’s Good Samaritan concept of its meaning.”²⁴

This sweeping grant of immunity has been the subject of widespread criticism and calls for reform.²⁵ Justice Clarence Thomas has called for the Supreme Court to review the scope of Section 230.²⁶ Ninth Circuit Judge Ryan Nelson recently stated that courts have “stretch[ed] the statute’s plain meaning beyond recognition,” leading to “perverse effects.”²⁷ The Ninth Circuit “should revisit our precedent,” he urged, particularly in light of “artificial intelligence raising the specter of lawless and limitless protections.”²⁸

Courts have emphasized, however, that Section 230 immunity is not limitless.²⁹ Under Ninth Circuit precedent, Section 230(c)(1) immunity exists for “(1) a provider or user of an interactive computer service (2) whom a plaintiff seeks to treat, under a state law cause of action, as a publisher or speaker (3) of information provided by another information content provider.”³⁰ While the first prong is rarely at issue – the term “interactive computer service” is broadly defined³¹ – the second and third prongs, which “tend to overlap in significant ways,”³² require courts to analyze the role a website plays in the offensive conduct.

With respect to the second prong, Section 230 does not immunize a website that is itself an “information content provider” who is “responsible, in whole or in part, for the creation or development of information” that is the source of liability.³³ In *Roommates.com*, the Ninth Circuit interpreted the phrase “creation or development in whole or in part” to mean that “a website helps to develop unlawful content . . . if it contributes materially to the alleged illegality of the conduct.”³⁴ The court held that a roommate-matching service acted as an information content provider, and thus enjoyed no immunity, when it required that users disclose protected characteristics that materially contributed to alleged violations of anti-discrimination laws. The court noted that, by contrast, “providing *neutral* tools to carry out what may be unlawful or illicit searches does not amount to ‘development’ for purposes of the immunity exception.”³⁵

²³ Michael Rustad & Thomas Koenig, “The Case for a CDA Section 230 Notice-and-Takedown Duty” (2023) 23 Nev.L.J. 533, 566.

²⁴ Danielle Keats Citron, “How to Fix Section 230” (2023) 103 B.U.L. Rev. 713, 727.

²⁵ 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>.

²⁶ *Doe ex rel. Roe v. Snap, Inc.* (2024) 144 S. Ct. 2493 (Thomas, J., dissenting from denial of certiorari).

²⁷ *Calise v. Meta Platforms, Inc.* (9th Cir. 2024) 103 F.4th 732, 747 (Nelson, J. concurring) (*Calise*).

²⁸ *Ibid.*

²⁹ *Calise*, *supra*, 103 F.4th at p. 739, citing cases.

³⁰ *Barnes v. Yahoo!, Inc.* (9th Cir. 2009) 570 F.3d 1096, 1109 (*Barnes*).

³¹ The term “interactive computer service” means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions. (42 U.S.C. § 230(f)(2).)

³² *In re Apple Inc. Litig.* (N.D.Cal. 2022) 625 F. Supp. 3d 971, 978.

³³ 42 U.S.C. § 230(f)(3).

³⁴ *Roommates.com*, *supra*, 521 F.3d at p. 1168.

³⁵ *Id.* at p. 1169, emphasis in original.

With respect to the third prong, Section 230 protection extends only to claims that “derive[] from the defendant’s status or conduct as a publisher or speaker.”³⁶ If, instead, the claim “springs from something separate from the defendant’s status as a publisher, such as from . . . obligations the defendant has in a different capacity,” Section 230 immunity does not apply.³⁷ Examples of such cases include:

- Yahoo’s promise and subsequent failure to remove revenge pornography and defamatory content, as the asserted liability derived from contract principles.³⁸
- A networking website owner’s unlawful failure to warn a woman who was raped by two users of the website who posed as talent scouts to lure her to a fake audition, where it was alleged that an outside source had informed the owner about the predatory scheme.³⁹
- A city ordinance that required short-term home rental websites to refrain from completing booking transactions for properties not registered with the city, and to refrain from collecting or receiving a fee for “facilitating or providing services ancillary to a vacation rental or unregistered home-share.”⁴⁰
- Snap’s allegedly defectively-designed app, which promoted content that encouraged two teen boys who died in a high-speed car accident to drive at dangerous speeds.⁴¹
- The claim that Google aided and abetted terrorism by sharing advertising revenue with ISIS.⁴²
- Platforms that processed payments for unlawful purchases of virtual chips for illegal casino apps.⁴³

While these cases are highly fact-specific, taken together they establish that Section 230 does not shield conduct, including sharing revenue or otherwise facilitating illegality, that can be characterized as the platform’s own unlawful act.⁴⁴ Section 230 is not “an all-purpose get-out-of-jail-free card”⁴⁵ that “create[s] a lawless no-man’s-land on the internet.”⁴⁶ The Ninth Circuit has “consistently eschewed an expansive reading of the statute that would render unlawful conduct ‘magically . . . lawful when [conducted] online,’ and therefore ‘giv[ing] online businesses an unfair advantage over their real-world counterparts.’”⁴⁷

Turning to this bill, nudification sites, unlike platforms that act as passive conduits for user-generated content, use GenAI to create realistic but false images of a victim’s likeness

³⁶ *Barnes*, *supra*, 570 F.3d at p. 1102.

³⁷ *Calise v. Meta Platforms, Inc.* (9th Cir. 2024) 103 F.4th 732, 742.

³⁸ *Barnes*, *supra*, 570 F.3d at p. 1109.

³⁹ *Doe v. Internet Brands, Inc.* (9th Cir. 2016) 824 F.3d 846, 852-853.

⁴⁰ *HomeAway.com, Inc. v. City of Santa Monica* (9th Cir. 2019) 918 F.3d 676, 682 (*HomeAway*).

⁴¹ *Lemmon v. Snap, Inc.* (9th Cir. 2021) 995 F.3d 1085, 1092.

⁴² *Gonzalez v. Google LLC* (9th Cir. 2021) 2 F.4th 871, 890 (*Gonzalez*). This case was eventually resolved on the grounds that the plaintiffs did not allege facts sufficient to show a violation of anti-terrorism laws.

⁴³ *In re Apple Inc. Litig.* (N.D.Cal. 2022) 625 F. Supp. 3d 971, 994.

⁴⁴ *See ibid.*

⁴⁵ *Doe v. Internet Brands, Inc.*, *supra*, 824 F.3d at p. 853.

⁴⁶ *HomeAway*, *supra*, 918 F.3d at p. 683.

⁴⁷ *Ibid.*, citation omitted.

incorporated into sexually explicit imagery or video. Thus, a strong argument can be made that nudification sites are “information content providers” because they create illegal content – image-based sexual abuse – or, at a minimum, materially contribute to illegal conduct.⁴⁸ As a result, Section 230 likely does not protect these sites.

As for platforms that knowingly or recklessly facilitate violations of the bill, section 230’s application will be determined on a case-by-case basis. Depending on the facts of a given case, plaintiffs may be able to successfully assert claims against entities that provide services that enable the operation of nudification websites because they are engaging in their own unlawful acts. In recognition of this issue, however, the bill provides that liability in this context applies “[e]xcept as provided by federal law.” Likewise, although cases have held Section 230 immunity applies to platforms whose recommendation algorithms curate and promote illicit content, multiple judges in the Ninth Circuit have argued that publisher immunity should not apply in such cases,⁴⁹ and last year the Third Circuit adopted this position in light of a recent Supreme Court decision.⁵⁰ The Ninth Circuit may well follow suit.

6) **Amendments.** The author has offered to amend the bill to clarify its scope by providing that in order for a website to qualify as a deepfake pornography service, producing such deepfakes must be the site’s primary purpose. The amendments also include a handful of clarifying and clean-up changes. The amendments are as follows:

SECTION 1. Section 1708.86 of the Civil Code is amended to read:

1708.86. (a) For purposes of this section:

(1) “Authorized Representative” means an attorney, talent agent, or personal manager authorized to represent a depicted individual if the depicted individual is represented.

(2) (A) “Consent” means an agreement written in plain language signed knowingly and voluntarily by the depicted individual that includes a general description of the digitized sexually explicit material and the visual or audiovisual work in which it will be incorporated.

(B) A depicted individual may rescind consent by delivering written notice within three business days from the date consent was given to the person in whose favor consent was made, unless one of the following requirements is satisfied:

⁴⁸ See Matt Perault, “Section 230 Won’t Protect ChatGPT Lawfare,” (February 22, 2023), <https://www.lawfaremedia.org/article/section-230-wont-protect-chatgpt>.

⁴⁹ See, e.g., *Force v. Facebook, Inc.* (2d Cir. 2019) 934 F.3d 53, 76 (Katzmann, C.J., concurring in part and dissenting in part); *Gonzalez, supra*, 2 F.4th at p. 913 (Berzon, J., concurring); *Calise, supra*, 103 F.4th at p. 747 (Nelson, J. concurring).

⁵⁰ *Anderson v. TikTok Inc.* (3d Cir. 2024) 116 F.4th 180, 184 184 held that TikTok’s recommendation algorithm—which promoted a “Blackout Challenge” to a 10-year-old girl who then died from self-asphyxiation—was the platform’s own expressive conduct that falls outside of section 230. The court drew on a recent Supreme Court holding that an algorithm that editorially curates third-party speech is protected by the First Amendment. (*Id.*, discussing *Moody v. NetChoice, LLC* (2024) 603 U.S. 707.) As to the interplay between section 230 and the First Amendment, the Third Circuit quoted Justice Thomas’s observation that “[i]n the platforms’ world, they are fully responsible for their websites when it results in constitutional protections, but the moment that responsibility could lead to liability, they can disclaim any obligations and enjoy greater protections from suit than nearly any other industry.” (*Doe ex rel. Roe v. Snap, Inc.* (2024) 144 S. Ct. 2493 (Thomas, J., dissenting from denial of certiorari).)

(i) The depicted individual is given at least 72 hours to review the terms of the agreement before signing it.

(ii) The depicted individual's authorized representative provides written approval of the signed agreement.

(3) "Deepfake pornography service" means an internet website, mobile application, or other service ~~that, through digitization, creates~~ ***the primary purpose of which is to create*** digitized sexually explicit material.

(4) "Depicted individual" means an individual who is portrayed in sexually explicit ~~material as a result of digitization.~~ ***material.***

(5) "Despicable conduct" means conduct that is so vile, base, or contemptible that it would be looked down on and despised by a reasonable person.

(6) "Digitization" means a process by which any of the following are realistically depicted:

(A) The nude body parts of another human being as the nude body parts of the depicted individual.

(B) Computer-generated nude body parts as the nude body parts of the depicted individual.

(C) The depicted individual engaging in sexual conduct in which the depicted individual did not engage.

(7) "Digitized sexually explicit material" means any portion of a visual or audiovisual work created or substantially altered through digitization, including an image, that shows the depicted individual in the nude or appearing to engage in, or being subjected to, sexual conduct.

(8) "Disclose" means to publish, make available, or distribute to the public.

(9) "Individual" means a natural person.

(10) (A) "Malice" means an intent to cause harm to the ~~plaintiff~~ ***depicted individual*** or to engage in despicable conduct with a willful and knowing disregard of the rights of the ~~plaintiff.~~ ***depicted individual.***

(B) A person acts with knowing disregard within the meaning of this paragraph when the person is aware of the probable harmful consequences of their conduct and deliberately fails to avoid those consequences.

(11) "Nude" means visible genitals, pubic area, anus, or a female's postpubescent nipple or areola.

(12) "Person" means a natural person or legal entity.

(13) "Plaintiff" includes cross-plaintiff.

(14) "Public prosecutor" means the Attorney General, a city attorney, county counsel, district attorney, or any other city or county prosecutor.

(15) "Sexual conduct" means any of the following:

(A) Masturbation.

(B) Sexual intercourse, including genital, oral, or anal, whether between persons regardless of sex or gender or between humans and animals.

(C) Sexual penetration of the vagina or rectum by, or with, an object.

(D) The transfer of semen by means of sexual conduct from the penis directly onto the depicted individual as a result of ejaculation.

(E) Sadomasochistic abuse involving the depicted individual.

(b) A depicted individual ~~who is at least 18 years of age~~ has a cause of action against a person who does any of the following:

(1) Creates and intentionally discloses digitized sexually explicit material portraying the depicted individual, and the person knows, or reasonably should ~~have known~~, **know**, that the depicted individual in that material did not consent to its creation or ~~disclosure~~. **disclosure or was a minor when the material was created.**

(2) Intentionally discloses digitized sexually explicit material portraying the depicted individual that the person did not create, and the person knows, or reasonably should ~~have known~~, **know**, that the depicted individual in that material did not consent to the creation of the digitized sexually explicit ~~material~~. **material or was a minor when the material was created.**

(3) Knowingly or recklessly facilitates, aids, or abets conduct prohibited by paragraph (1) or (2).

~~(c) A depicted individual who is a minor has a cause of action against a person who does either of the following:~~

~~(1) Creates or intentionally discloses digitized sexually explicit material portraying the depicted individual.~~

~~(2) Knowingly or recklessly facilitates, aids, or abets conduct prohibited by paragraph (1).~~

~~(d)~~(c) For purposes of this section, both of the following apply:

(1) A person that owns, operates, or controls a deepfake pornography service is engaged in the creation and intentional disclosure of digitized sexually explicit material and is presumed to know that the depicted individual did not consent to the creation or disclosure of the digitized sexually explicit material, unless the person produces evidence of the depicted individual's express written consent.

(2) ~~Except as provided by federal law, a~~ A person that knowingly or recklessly provides a service that enables the operation of a deepfake pornography service is ~~engaged in knowing and reckless facilitation, aiding, or abetting as described in~~ **presumed to be in violation of** paragraph (3) of subdivision (b) ~~and paragraph (2) of subdivision (c) and is presumed to act with knowledge or recklessness with respect to providing the service~~ if both of the following are true:

(A) A plaintiff provided the person with evidence demonstrating that ~~an internet website or mobile application served by~~ the person is **was providing services to** a deepfake pornography service that engages in conduct that violates this section.

(B) The person failed to stop providing services to the ~~internet website or mobile application~~ **deepfake pornography service** within 30 days of receiving the evidence described in subparagraph (A).

~~(c)(d)~~ (1) A person is not liable under this section in either of the following circumstances:

(A) The person discloses the digitized sexually explicit material in the course of any of the following:

- (i) Reporting unlawful activity.
- (ii) Exercising the person's law enforcement duties.
- (iii) Hearings, trials, or other legal proceedings.

(B) The material is any of the following:

- (i) A matter of legitimate public concern.
- (ii) A work of political or newsworthy value or similar work.
- (iii) Commentary, criticism, or disclosure that is otherwise protected by the California Constitution or the United States Constitution.

(2) For purposes of this subdivision, digitized sexually explicit material is not of newsworthy value solely because the depicted individual is a public figure.

~~(f)~~ (e) (1) It shall not be a defense to an action under this section that there is a disclaimer included in the digitized sexually explicit material that communicates that the depicted individual did not participate in or authorize the creation or development of the material.

(2) It shall not be a defense to an action under this section that a deepfake pornography service has a disclaimer or statement that states that users are prohibited from generating digitized sexually explicit material of a depicted individual without the individual's consent.

~~(g)~~ (f) (1) A prevailing plaintiff who is a depicted individual who suffers harm as a result of a violation of this section may recover any of the following:

(A) An amount equal to the monetary gain made by the defendant from the creation, development, or disclosure of the digitized sexually explicit material.

(B) One of the following:

(i) Economic and noneconomic damages proximately caused by the disclosure of the digitized sexually explicit material, including damages for emotional distress.

(ii) Upon request of the plaintiff at any time before the final judgment is rendered, the plaintiff may instead recover an award of statutory damages for all unauthorized acts involved in the action, with respect to any one work, as follows:

(I) A sum of not less than one thousand five hundred dollars (\$1,500) but not more than fifty thousand dollars (\$50,000).

(II) If the unlawful act was committed with malice, the award of statutory damages may be increased to a maximum of ~~one~~ two hundred fifty thousand dollars ~~(\$150,000)~~ (\$250,000).

(C) Punitive damages.

(D) Reasonable attorney's fees and costs.

(E) Any other available relief, including injunctive relief.

(2) A public prosecutor may bring a civil action to enforce this section.

(A) In an action brought under this paragraph, the public prosecutor shall not be required to prove that a depicted individual suffered actual harm.

(B) A prevailing public prosecutor under this paragraph is entitled to all of the following:

(i) Injunctive and other equitable relief.

(ii) A civil penalty of twenty-five thousand dollars (\$25,000) per violation.

(iii) For a violation committed with malice, a civil penalty of fifty thousand dollars (\$50,000) per violation.

(iv) Reasonable attorney's fees.

(v) Any other relief the court deems appropriate.

(3) The remedies provided by this section are cumulative and shall not be construed as restricting a remedy that is available under any other law.

~~(h)~~ (g) An action under this section shall be commenced no later than three years from the date the unauthorized creation, development, or disclosure was discovered or should have been discovered with the exercise of reasonable diligence.

~~(i)~~ (h) The provisions of this section are severable. If any provision of this section or its application is held invalid, that invalidity shall not affect other provisions.

(i) *This section does not apply to conduct that is protected by federal law.*

ARGUMENTS IN SUPPORT: San Francisco City Attorney David Chiu, the bill’s sponsor, writes:

In August 2024, my office announced a first-of-its-kind lawsuit against some of the world’s largest websites that create and distribute nonconsensual AI-generated pornography. Our lawsuit alleges violations of state and federal laws prohibiting deepfake pornography, revenge pornography, and child pornography, as well as violations of California’s Unfair Competition Law. My office pursues public interest cases under California’s Unfair Competition Law to protect consumers and ensure fair competition among businesses. We have successfully litigated a range of consumer protection cases targeting unlawful and deceptive practices across a variety of industries.

Even though existing law prohibits the creation and distribution of nonconsensual AI-generated pornography, and public prosecutors have broad enforcement powers that enable them to sue operators of websites that create such imagery, there are significant enforcement gaps within existing law. Crucially, it does not apply to entities that facilitate the operation of such websites, allowing enablers of bad actors to profit off deepfake pornography with impunity. Additionally, the civil penalties public prosecutors can recover through their general enforcement powers are relatively small, limiting the deterrent effect of these laws.

AB 621 augments the existing statute that provides civil liability for the intentional creation and distribution of deepfake pornography by expressly applying it to deepfake pornography websites, expanding it to apply to those who knowingly or recklessly facilitate the operation of such websites or the creation or distribution of such images, expressly giving standing to public prosecutors to take enforcement actions under the statute, and increasing the amount of damages and penalties that violators may face.

The California District Attorneys Association, in support, writes:

The proliferation of deepfake technology has led to a disturbing rise in digitally manipulated sexually explicit content, often used to harass, exploit, and defame individuals—particularly women and minors. While existing law provides victims with a cause of action against those who create or distribute such material, AB 621 strengthens these protections by extending liability to those who knowingly facilitate, aid, or abet the distribution of deepfake pornography. The bill also increases statutory damages for victims and provides a mechanism for public prosecutors to pursue civil enforcement actions.

By holding accountable both creators and enablers of this abusive content, AB 621 closes critical loopholes in current law and ensures that victims have meaningful legal recourse. Furthermore, by allowing for public enforcement actions, the bill empowers law enforcement agencies to take proactive steps against bad actors operating deepfake pornography services.

ARGUMENTS IN OPPOSITION: In opposition to the bill, California Civil Liberties Advocacy writes:

On the whole, AB 621 appears to be a comprehensive expansion of California’s legal protections against deepfake pornography, addressing technological advancements and closing loopholes in current law, which the CCLA generally supports. While it is well-positioned to strengthen victim protections and hold bad actors accountable, it may face legal challenges regarding free speech, platform liability, and enforcement scope. Further

refinements may be needed to ensure compliance with federal law, avoid unintended burdens on service providers, and circumvent potential chilling effects.

REGISTERED SUPPORT / OPPOSITION:

Support

San Francisco City Attorney's Office (UNREG) (Sponsor)
California District Attorneys Association
Consumer Attorneys of California
Joyful Heart Foundation

Oppose Unless Amended

California Civil Liberties Advocacy

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