Date of Hearing: June 16, 2026
Fiscal: No

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
SB 1111 (Ashby) – As Amended March 23, 2026

SENATE VOTE: 36-0

SUBJECT: Digital replicas

SYNOPSIS

The advent of generative artificial intelligence (GenAI) has led to the widespread availability of consumer-facing website and mobile applications capable of readily creating digital replicas – highly-realistic imagery and video using another person's voice or likeness – that can depict a person, without their consent, engaging in conduct they never actually engaged in. This has led to a proliferation of deepfakes, including scams and pornography, which can have devastating impacts on the depicted individuals.

This measure seeks to ensure California's legal framework keeps pace with these developments. First, the bill provides that the state's "right of publicity" law governing the commercial misappropriation of a person's name, image, or likeness applies to digital replicas. The bill also eliminates an outdated evidentiary presumption that shields incidental use of an employee's likenesses. Second, the bill amends the Penal Code to specify that use of a digital replica with intent to impersonate a person constitutes false impersonation under existing criminal statutes. The bill is similar to SB 11 (Ashby, 2025), which was vetoed by the Governor on the basis of a consumer warning requirement that is not in this year's bill.

The bill is sponsored by 11:11 Media and supported by, among others, the California Initiative for Technology and Democracy, the California Federation of Labor Unions, SAG-AFTRA, and Rape, Abuse, & Incest National Network (RAINN).

If passed by this Committee, the bill will be re-referred to the Judiciary Committee.

EXISTING LAW:

1) Defines:

    a. "Artificial intelligence" 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. (Civ. Code § 3110.)

    b. "Digital replica" as a computer-generated, highly realistic electronic representation that is readily identifiable as the voice or visual likeness of an individual that is embodied in a sound recording, image, audiovisual work, or transmission in which the actual individual either did not actually perform or appear, or the actual individual did perform or appear, but the fundamental character of the performance or appearance has been materially altered. Excludes electronic reproduction, use of a

sample of one sound recording or audiovisual work into another, remixing, mastering, or digital remastering of a sound recording or audiovisual work authorized by the copyright holder from the definition. (Civ. Code § 3344.1.)

2) Provides that any person who knowingly uses another's name, voice, signature, photograph or likeness, in any manner, on or in products, merchandise, or goods, or for the purposes of advertising or selling, or soliciting purchases of, products, merchandise, goods or services, without such person's prior consent, is liable for statutory damages, actual damages, lost profits, punitive damages, and attorney's fees and costs. (Civ. Code § 3344(a).)

3) Provides that where a photograph or likeness of an employee of the person using the photograph or likeness appearing in the advertisement or other publication prepared by or on behalf of the user is only incidental, and not essential, to the purpose of the publication in which it appears, there is a rebuttable presumption affecting the burden of producing evidence that the failure to obtain consent of the employee was not a knowing use of the employee's photograph or likeness. (Civ. Code § 3344(c).)

4) Provides that any person who knowingly and without consent credibly impersonates another actual person through or on a website or by other electronic means for purposes of harming, intimidating, threatening, or defrauding another person is guilty of a public offense punishable by a fine and/or imprisonment. (Pen. Code § 528.5.)

5) Provides that every person who falsely personates another in either his or her private or official capacity, and in that assumed character does certain listed acts, is subject to a fine and/or imprisonment. (Pen. Code § 529.)

6) Provides that every person who falsely impersonates another, in either their private or official capacity, and in such assumed character receives any money or property, knowing that it is intended to be delivered to the individual so personated, with intent to convert the same to their own use, or to that of another person, or to deprive the true owner thereof, is punishable in the same manner and to the same extent as for larceny of the money or property so received. (Pen. Code § 530.)

THIS BILL:

1) Provides, for purposes of California's "right of publicity" law under Civil Code section 3344, that a person's voice or likeness includes a digital replica.

2) Removes a rebuttable presumption under section 3344(c), as described above.

3) Provides that Penal Code provisions governing false impersonation include the use of a digital replica with the intent to impersonate another.

COMMENTS:

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

California is leading the nation in AI regulations. However, a significant gap remains. The lack of a comprehensive legal framework to address the non-consensual creation of AI deepfake images leaves victims with no remedy. While some deepfakes target public figures,

AI software now allows users to create content featuring anyone. Often, women are the targeted victims, and the vast majority of incidents are sexually explicit in nature.

SB 1111 creates a framework to hold AI users accountable by establishing clear legal standing for victims and defining the boundaries of AI technology. As technology changes, California must continue to advance the standard for protections against AI violence and those affected by it.

2) **Background**. *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 is capable of processing, including numbers, text, audio, video, and 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.

Digital replicas. Technological advances have had major implications for likeness rights. The term "digital replicas" is used to describe computer-generated avatars of an individual's likeness—including their face, body, voice, movement; indeed, their very identity—that can appear authentic but be manipulated to create entirely new "performances," even if the actor had no active role in the making of the performance. For example, James Dean, despite passing away over 60 years ago, was cast in a 2019 movie using a digital replica.[2]

Meanwhile, "[a]spiring musicians, actors, and models routinely sign predatory blanket, long-term (sometimes perpetual) assignments and licenses of their publicity rights as a condition of getting representation, a record deal, a role, or a photo shoot," writes Professor Jennifer Rothman, a leading scholar on the issue. "Similarly, the NCAA has had student-athletes sign contracts as a condition of participation in college athletics that the NCAA claimed assigned to it the perpetual rights to those students' names and likenesses for use in any context."[3]

Last session, two bills enacted protections related to digital replicas in the entertainment industry. AB 2602 (Kalra, Stats. 2024, Ch. 259) deemed unenforceable contractual provisions governing digital replicas that (1) do not sufficiently delineate the uses of the digital replica, or (2) for which the performer lacked proper representation, either by an attorney or labor union

---

[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] "James Dean set to star in new film through digital resurrection, horrifying fans" (Nov. 7, 2019) *NBC News*, https://www.nbcnews.com/pop-culture/celebrity/james-dean-set-star-new-film-through-digital-resurrection-horrifying-n1078051.

[3] Jennifer E. Rothman, *The Right of Publicity: Privacy Reimagined for a Public World* (Harvard University Press, 2018), p. 117.

representative. Additionally, to prevent the unauthorized reanimation of dead celebrities, AB 1836 (Bauer-Kahan, Stats. 2024, Ch. 258) established a specific cause of action for beneficiaries of deceased celebrities for the unauthorized use of a digital replica of the celebrity in audiovisual works or sound recordings.

Deepfake pornography. 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,[4] 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.[5]

In February 2024, deepfake nude images of 16 eighth-grade students were circulated among students at a California middle school.[6] Similar reports of abuses, almost always against girls, have been reported across the country and show no sign of abating.[7] In the first six months of 2024, some of the most popular nudification websites had been visited over 200 million times.[8] 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

---

[4] 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/.
[5] 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.
[6] 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.
[7] 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/studentsare-sharing-sexually-explicit-deepfakes-are-schools-prepared/2024/09; Gabrielle Hunt and Daryl Higgens "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.
[8] *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.

via social media.[9] 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.[10]

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.[11] 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.[12] 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 deepfake pornographic content is becoming normalized and accepted. Further, of those surveyed almost one-third stated they did not think deepfake pornography hurt anyone as long as it was only used for their personal interest.[13]

In August of 2024, San Francisco City Attorney David Chiu filed a lawsuit against 16 nudification websites.[14] 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.[15] Added by AB 602 (Berman, 2019), section 1708.86 grants a cause of action for an individual depicted in deepfake

---

[9] 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.
[10] 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.
[11] 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.
[12] *Ibid.*
[13] *2023 State of Deepfakes: Realities, Threats, and Impact*, Home Security Heroes, https://www.homesecurityheroes.com/state-of-deepfakes/#deepfake-porn-survey.
[14] Chase DiFeliciantonio, "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.
[15] *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.

pornography against a person who intentionally creates or discloses the deepfake pornography without the consent of the individual. AB 621 (Bauer-Kahan, Stats. 2024, Ch. 673) updated this statute to, among other things, expressly apply to nudification websites.

False impersonation. Speech and video created by GenAI is also driving a new era in scamming. These GenAI tools are trained on publicly available data – the more data a target has online, the easier it is to develop a passable imitation of them or their loved ones. This is especially true of wealthy individuals, whose public appearances, including speeches, are often widely available on the internet.[16]

As an example, a complicated scam utilizing both deepfake video and false audio was performed in Hong Kong in early 2024. A multinational company lost $25.6 million after employees were fooled by deepfake technology, with one incident involving a digitally recreated version of its chief financial officer ordering money transfers in a video conference call. Everyone present on the video call, except the victim, was a fake representation of real people. The scammers applied deepfake technology to turn publicly available video and other footage into convincing versions of the meeting's participants.[17]

AI technology has also been used to impersonate elected officials. In January 2024, between 5,000 and 20,000 New Hampshire residents received AI-generated phone calls impersonating President Biden that told them not to vote in the state's primary.[18] The call told voters: "It's important that you save your vote for the November election." It remains unclear how many people might not have voted based on these calls.

3) **What this bill would do.** This bill seeks to update California's civil and criminal laws relating to likeness rights and false impersonation in order to keep pace with the challenges posed by GenAI. Existing Civil Code section 3344 codifies the right to publicity, imposing liability on any person who knowingly uses another's name, voice, signature, photograph, or likeness, in any manner, on or in products, merchandise, or goods, or for purposes of advertising or selling, or soliciting purchases of, products, merchandise, goods or services, without prior consent.[19] Additionally, existing law prohibits the false impersonation of another person in either their personal or official capacity with the intent to steal or defraud. This bill updates those laws to clarify they apply to digital replicas.

Furthermore, SB 1111 eliminates a rebuttable presumption providing that an employer does not knowingly violate a deceased personality's publicity rights if the use of their likeness is incidental to a publication and part of the employee's job. The presumption, which dates back to 1971, is outdated given the ease with which photographs can now be digitally edited.

---

[16] Emily Flitter and Stacy Cowley, "Voice Deepfakes Are Coming for Your Bank Balance," New York Times, August 30, 2023, www.nytimes.com/2023/08/30/business/voice-deepfakes-bank-scams.html.
[17] Harvey Kong, "Everyone looked real': multinational firm's Hong Kong office loses HK$200 million after scammers stage deepfake video meeting," South China Morning Post, February 4th, 2024, www.scmp.com/news/hong-kong/law-and-crime/article/3250851/everyone-looked-real-multinational-firms-hong17kong-office-loses-hk200-million-after-scammers-stage.
[18] Cat Zakrzewski and Pranshu Verma, "New Hampshire opens criminal probe into AI calls impersonating Biden," *Washington Post*, Feb. 6, 2024, www.washingtonpost.com/technology/2024/02/06/nh-robocalls-ai-biden/.
[19] Stats. 1971, Ch. 1595.

The bill is similar to last year's SB 11 (Ashby), which was vetoed by the Governor on the basis of a consumer warning requirement that is not in this year's bill.

ARGUMENTS IN SUPPORT: 11:11 Media, sponsor of the bill, writes:

> As artificial intelligence tools become more advanced and more accessible, it has become far too easy to create and spread nonconsensual AI-generated content. A person's voice or likeness can now be copied, manipulated, and used without their knowledge or consent. This abuse can be used to humiliate, harass, exploit, and impersonate people, causing serious emotional, reputational, and financial harm.
>
> This issue is urgent. AI-generated abuse is already being used to create sexually explicit deepfakes, spread false statements, and impersonate real people in deeply harmful ways. California's Department of Justice cites research showing that 90% of victims are women, 93% suffered significant emotional distress, 51% had suicidal thoughts, and 49% reported being stalked or harassed online by people who saw the material. These harms disproportionately affect women and girls and increasingly affect children as well.

REGISTERED SUPPORT / OPPOSITION:

Support

11:11 Media Impact (Sponsor)
California Federation of Labor Unions, Afl-cio
California Initiative for Technology & Democracy, a Project of California Common CAUSE
Common Sense Media

Opposition

None on file.

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