Date of Hearing: July 16, 2025
Fiscal: Yes

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
SB 11 (Ashby) – As Amended July 10, 2025

SENATE VOTE: 38-0

PROPOSED AMENDMENTS

SUBJECT: Artificial intelligence technology

SYNOPSIS

The advent of generative artificial intelligence (GenAI) has led to the widespread availability of consumer-facing website and mobile applications that can readily create 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 author-sponsored 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 The bill also eliminates an outdated evidentiary presumption that shields incidental use of an employee's likenesses.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. Third, the bill directs the Judicial Council to study the evidentiary challenges posed by AI-generated content and to develop rules of court to guide its admissibility, authentication, and use. Finally, the bill requires entities that make available to consumers AI tools capable of producing digital replicas to provide a consumer warning that unlawful use of the tool to depict another person without prior consent may result in potential civil or criminal liability for unlawful use.

The bill is supported by a broad coalition of entertainment unions and digital policy advocates, including SAG-AFTRA and Common Sense Media. It is opposed by trade associations, the tech industry, and the Chamber of Commerce, among others. The bill passed the Judiciary Committee on an 11-0 vote and the Public Safety Committee on a 9-0 vote.

A clarifying amendment is described in Comment #8.

THIS BILL:

1) Requires, by December 1, 2026, that any person or entity that makes available to consumers artificial technology capable of creating a digital replica provide a consumer warning that unlawful use of the technology to depict another without prior consent may result in civil or criminal liability for the user.

2) Requires that the warning be displayed to the consumer before their first use of the technology and thereafter be hyperlinked to from any page or screen where the consumer may input a prompt to the artificial intelligence technology. All warnings must be displayed in a manner that is clear and conspicuous.

3) Makes the provisions above enforceable by public prosecutors who may seek a civil penalty of $25,000 per violation.

4) 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.

5) Removes a rebuttable presumption under section 3344(c), as described below.

6) Requires, by January 1, 2027, the Judicial Council to review the impact of artificial intelligence on the admissibility of proffered evidence in court proceedings and develop any necessary rules of court to assist courts in assessing claims that proffered evidence has been generated by or manipulated by artificial intelligence and determining whether such evidence is admissible.

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

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.)

7) Grants the Judicial Council rulemaking authority to adopt rules of court to implement procedures and standards governing admissibility, including new rules to address technological changes affecting evidentiary practices. (Cal. Const., art. VI, § 6; Gov. Code § 68511; California Rules of Court, Title 10.)

COMMENTS:

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

> Artificial intelligence has pushed the boundaries of how technology makes human lives easier. However, the lack of necessary regulations has led to its abuse. Bad actors are creating and sharing AI deepfake videos, images, and audio recordings that use a person's name, image, or likeness without their consent. An alarming number of these deepfakes depict people engaging in sexual activities. This leaves victims vulnerable to exploitation including identity theft, scams, misinformation, and drastic misrepresentation of character. While some deepfakes target public figures, AI software allows users to create non-consensual content featuring anyone. This issue has disproportionately impacted women and girls, though not exclusively.
>
> Existing law does not allow victims to pursue private legal action when someone uses their likeness for AI generated material without their consent. SB 11 closes this gap by granting individuals the right to initiate litigation against those who use AI to falsely impersonate them and further requires courts to evaluate evidence generated by AI to ensure authenticity of evidentiary materials presented in our judicial system to a judge or jury. It also requires consumer warnings on AI software, both identifying and discouraging its potential for misuse. This bill strikes a balance between regulating rapidly advancing AI technologies and allowing continued innovation in the AI sector.

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) **Digital replicas.** Technological advances have had major implications for likeness rights. "Digital replicas" is the term for computer-generated avatars of an individual's likeness—including their face, body, voice, movement; indeed, their very identity—that can appear authentic and 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 (1) that 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 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.

4) **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.

---

[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.

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 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:

---

[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.

[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.

> 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 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.[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 pornography against a person who intentionally creates or discloses the deepfake pornography without the consent of the individual. AB 621 (Bauer-Kahan) would update this statute to, among other things, expressly apply to nudification websites.

5) **False impersonation.** Speech and video created by GenAI is also driving a new era in scamming. These Gen AI 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

---

[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.

especially true of wealthy clients, 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." Concern about this call has led at least 14 states to introduce legislation targeting AI-powered disinformation. It is still unclear how many people might not have voted based on these calls.

6) **What this bill would do.** This bill seeks to update California's legal framework to keep pace with the challenges posed by GenAI by doing the following:

> *Updating civil and criminal laws relating to likeness rights and false impersonation:* 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 11 eliminates a rebuttable presumption that an employer did not knowingly violate a deceased personality's publicity rights if the use of their likeness was incidental to a publication and part of the employee's job. The presumption, which traces back to 1971, is outdated given the ease with which photographs can now be digitally edited.
>
> *Updating evidentiary rules:* The bill requires, by January 1, 2027, the Judicial Council to review the impact of artificial intelligence on the admissibility of evidence in court proceedings and develop any necessary rules of court to assist courts in identifying AI-generated evidence and determining whether it should be admitted. According to the Judiciary Committee's analysis of the bill:

---

[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.

> SB 11's Judicial Council study thus responds to a critical and timely concern: that without clearer guidance, the legal system may admit fabricated or unverifiable evidence under the guise of technological sophistication, eroding the integrity of judicial fact-finding. The study's outcome could form the basis for future rulemaking under the California Rules of Court or legislative reform of the Evidence Code. Given the accelerating deployment of generative AI in civil and criminal litigation—from predictive algorithms used to establish probable cause to synthetic exhibits and deepfake impersonation—the legal system is under pressure to develop new evidentiary tools.[20]

Consumer warning: In order raise awareness about the legal consequences of misuse of digital replicas, the bill requires a warning to be displayed to users of AI tools that can create digital replicas. The warning states that "Unlawful use of this technology to depict another person without prior consent may result in civil or criminal liability for the user." The warning must be displayed to the consumer before their first use of the technology and thereafter be hyperlinked to from any page or screen where the consumer may input a prompt to the AI technology. Warnings must be displayed in a manner that is clear and conspicuous. Violations of these requirements are punishable by a civil penalty of up to $25,000, enforceable by public prosecutors.

7) **Compelled speech.** "The First Amendment's guarantee of freedom of speech makes no distinction of 'constitutional significance' 'between compelled speech and compelled silence.'"[21] By requiring providers of AI tools capable of creating digital replicas to display a consumer warning that unlawful use of such tools to depict another person without their consent may result in civil or criminal liability, the bill, as opponents note, implicates the First Amendment.

Warning labels, a long-standing and widespread staple of consumer protection, have been applied to numerous commercial products, including on nutritional labels for foods, health inspection results for restaurants, and warnings on products containing tobacco, alcohol, pharmaceuticals, toxins, flammable or corrosive substances, and carcinogens.[22] Such warnings enjoy a much more lenient standard of judicial scrutiny – "akin to a rational basis test"[23] – than other forms of First Amendment infringements. Under this standard, set forth in *Zauderer v. Office of Disciplinary Counsel* (1985) 471 U.S. 626, the warning label must contain "'purely factual and uncontroversial information'"[24] and must not be "unduly burdensome."[25]

---

[20] Asm. Jud. Analysis Sen. Bill No. 11 (2025-2026 Reg. Sess.) at p. 8.
[21] *X Corp. v. Bonta* (9th Cir. 2024) 116 F.4th 888, 900.
[22] *See Symposium: Compelled Speech: The Cutting Edge of First Amendment Jurisprudence: Compelled Speech and the Regulatory State* (2022) 97 Ind. L.J. 881, 894-895.
[23] *X Corp. v. Bonta, supra,* 116 F.4th at p. 900, quoting *Nat'l Ass'n of Wheat Growers v. Bonta* (9th Cir. 2023) 85 F.4th 1263, 1266 (*Wheat Growers*).
[24] *CTIA - The Wireless Ass'n v. City of Berkeley* (9th Cir. 2019) 928 F.3d 832, 842 (*CTIA*), quoting *Zauderer v. Off. of Disciplinary Couns. of Sup. Ct. of Ohio* (1985) 471 U.S. 626, 651 (*Zauderer*); *Am. Bev. Ass'n v. City & Cty. of San Francisco* (9th Cir. 2019) 916 F.3d 749, 756 ("*Zauderer* provides the appropriate framework to analyze a First Amendment claim involving compelled commercial speech . . . when the government requires health and safety warnings"); *Nat'l Inst. of Fam. and Life Advocs. v. Becerra* (2018) 585 U.S. 755, 775 (*NIFLA*) (stating that "we do not question the legality of health and safety warnings long considered permissible, or purely factual and uncontroversial disclosures about commercial products"); *X Corp. v. Bonta* (9th Cir. 2024) 116 F.4th 888, 901 ("retail product warnings" are "characterized . . . as commercial speech" even though they are "not a clear fit" with the general rule that commercial speech involves speech that proposes a commercial transaction); *see also Chamber*

According to the Judiciary Committee analysis of the prior version of the bill, which is substantially similar to the current version, "SB 11's disclosure requirement fits within the *Zauderer* framework, does not burden expressive conduct, and is narrowly tailored to address the documented risks of AI-generated impersonations."[26]

8) **Clarifying amendment**. The author has agreed to the following clarifying amendment:

> **22650.** (a) By December 1, 2026, any person or entity that makes available to consumers any artificial intelligence technology that ~~is capable of creating any~~ ***enables a user to create*** a digital replica shall provide the following consumer warning:
>
> > "Unlawful use of this technology to depict another person without prior consent may result in civil or criminal liability for the user."

ARGUMENTS IN SUPPORT: The Center for AI and Digital Policy writes:

> The rapid development of AI has enabled the creation of highly realistic digital replicas known as "deepfakes," which can make it appear as though someone said or did something they never did. Often used maliciously, deepfakes spread false information, create non-consensual explicit content, and impersonate individuals for fraud and harassment.
>
> Deepfakes cause immediate and lasting damage to reputations, careers, and personal relationships. Once circulated, they are nearly impossible to erase, leaving victims with little recourse and long-term emotional, social, and financial harm. The number and sophistication of attacks targeting consumers is rising sharply. For example, in January, a deepfake audio clip falsely portraying a school principal making racist and antisemitic remarks went viral, leading to death threats and administrative leave, only to later be traced to a school employee under investigation.
>
> In April 2023, scammers used AI to clone a 15-year-old girl's voice in a fake kidnapping call to her mother.8 Another victim, an 82-year-old retiree, lost $690,000 after being deceived by a deepfake video of Elon Musk. These cases show how deepfakes inflict rapid, often irreversible harm to a person's reputation, safety, and financial security. (Emphasis and footnotes omitted.)

Common Sense Media writes:

> AI capabilities have shown how detrimental its misuse can be when there is malicious intent. AI manipulated content continues to harm victims across the state, with examples ranging from fake audio of elected officials making false statements, to synthetic material of primarily women engaging in sexual activities. While some deep fakes target public figures, easily accessible AI software now allows users to create non-consensual content featuring anyone. This issue predominately impacts women and girls and has been difficult for victims to address, much less seek justice.

---

of Commerce of United States v. United States SEC (5th Cir. 2023) 85 F.4th 760, 768 ("[s]tates may require commercial enterprises to disclose 'purely factual and uncontroversial information' about their services").
[25] *Zauderer, supra,* 471 U.S. at p. 651.
[26] Asm. Jud. Analysis Sen. Bill No. 11 (2025-2026 Reg. Sess.) at p. 6; emphasis in original.

ARGUMENTS IN OPPOSITION: A coalition led by California Chamber of Commerce writes in opposition to the prior version of the bill, which was recently amended in a way that addresses some of the concerns raised by the coalition. Issues of continuing relevance described in the coalition letter include:

> **First,** as drafted, the bill intends to capture business to business activities, such as companies selling advertising services to other companies wherein the advertisement may include a digital replica, as well as internal usage of tools, such as a marketing staff person developing a training video and includes a digital likeness of the Chief Training officer. To that end, we proposed amendments to exempt business-to-business activities as well as employees, but that was rejected by the author. As an alternative, we propose Section 22650 be amended to exempt business partners / vendors and employees when acting in their course of conduct where they have consent from the individual whose likeness will be used.
>
> [. . .]
>
> To that end, our **third** amendment proposes to limit the warning to those applications specifically designed and marketed to create "digital replicas". We believe such an amendment will ensure that the bill applies to tools that are designed explicitly to create realistic digital imitations of people's faces, voices, or likenesses and which advertises or highlights these replica capabilities, rather than sweeping in general-purpose AI tools that can technically be used to create replicas, but do not explicitly market that as a core function, because they have other use cases.
>
> [. . .]
>
> Specifically, we are concerned that the change to subdivision (f) of Section 3344 could lead to a perverse outcome where studios could be penalized for using a digital replica if a reasonable person believes it sounds like a real person even if that similarity was completely unintentional. Once a studio is put on notice that a reasonable person would believe the digital replica sounds like a real person, we would be violating section 3344(a), which prohibits the "knowing use of another's name, voice, signature, photograph, or likeness, in any manner […] without such person's prior consent[…]."
>
> Take for example if a studio uses a digital replica in a production that happens to sound like an individual it has never even heard of, and that the studio was not intentionally trying to copy. That individual could claim any profits from the studio that is attributable to the digital replica.
>
> [. . .]
>
> Our final and **fifth** amendment seeks to address the exceedingly high liability for businesses if the required consumer warning is not displayed to users. Currently, the bill seeks a penalty not to exceed $25,000 for each day that the technology is provided to or offered to the public without a consumer warning. Our proposed amendment is to lower this penalty to not exceed $5,000 a day.

REGISTERED SUPPORT / OPPOSITION:

Support

California Civil Liberties Advocacy
California District Attorneys Association
Chamber of Progress
Common Sense Media
Los Angeles County Democratic Party
National Ai Youth Council
Recording Industry Association of America (RIAA)
Sag-aftra
The Center for Ai and Digital Policy
Transparency Coalition.ai

Oppose Unless Amended

Association of National Advertisers
Calbroadband
California Chamber of Commerce
California Hispanic Chambers of Commerce
Computer and Communications Industry Association
Entertainment Software Association
Network Advertising Initiative
Software Information Industry Association
Technet
The Media Coalition

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