

SENATE JUDICIARY COMMITTEE
Senator Thomas Umberg, Chair
2025-2026 Regular Session

SB 1142 (Becker)
Version: April 8, 2026
Hearing Date: April 21, 2026
Fiscal: Yes
Urgency: No
AWM

SUBJECT

Digital Dignity Act

DIGEST

This bill requires a provider of a generative AI (GenAI) tool that is also a large online platform, as defined, and that allows users to create digital replicas, as defined, to create a mechanism for users to revoke access to their digital replica; requires a platform's terms of service to prohibit unlawful digital replicas, as specified; requires a platform to establish a mechanism to report unlawful digital replicas and a process to respond to such reports; and provides enhanced liability for a person who distributes content including a digital replica, with actual knowledge that the content includes a digital replica, and was either found liable for defamation for distributing the content or is in violation of specified criminal laws.

EXECUTIVE SUMMARY

"Digital replicas" are computer-generated, highly realistic electronic representations that are readily identifiable as the voice or visual likeness of an individual 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. The ultra-realism of digital replicas makes it easier than ever to fool members of the public with AI-generated images, videos, and sounds. It is also easier than ever to use AI-generated content to harass, abuse, or humiliate people online; as is often the case on the internet, women and girls, racial and sexual minorities, and gender nonconforming individuals have borne the brunt of this abuse.

The Legislature has enacted a number of bills to address the use of digital replicas and deepfakes. However, continuing concerns about the creation and distribution of nonconsensual digital replicas, including nonconsensual intimate imagery, highlight that existing laws may not adequately protect persons from false impersonation

resulting from the use of digital replicas that are created using GenAI on large online platforms. As currently drafted, this bill seeks to fill the gap by requiring GenAI platforms to provide mechanisms where a person can (1) revoke consent for the use of their digital removal and remove content involving their digital replica, and (2) report digital replicas created in violation of a revocation of consent. The bill also provides a heightened remedy available when a person suffers injury as the result of an unauthorized, unlawful use of a digital replica. In light of concerns that this mechanism could overly restrict constitutionally protected speech, the author has agreed to remove many of the provisions relating to the revocation of consent to use a digital replica and requiring an online platform to remove content. The author has also agreed to amendment to clarify the scope of the enhanced civil remedy.

This bill is sponsored by the Transparency Coalition and is supported by the California Institute for Technology & Democracy; the California Orthopaedic Association; the California Podiatric Medical Association; the California Society of Pathologists; CFT – A Union of Educators & Classified Professionals, AFT, AFL-CIO; Kapur Center Advocacy; and the Music Artists Coalition. This bill is opposed by the California Chamber of Commerce; the Civil Justice Association of California; the Computer & Communications Industry Association; Internet Works; the Motion Picture Association; Oakland Privacy; and TechNet. The Senate Privacy, Digital Technologies, and Consumer Protection Committee passed this bill with a vote of 7-0.

PROPOSED CHANGES TO THE LAW

Existing constitutional law:

- 1) Provides that the U.S. Constitution, the laws of the United States, and treaties made by the United States are the supreme law of the land. (U.S. Const., art. VI, cl. 2.)
- 2) Provides that Congress shall make no law abridging the freedom of speech, or the right of the people to peaceably assemble, and to petition the government for redress of grievances. (U.S. Const., 1st amend. (the First Amendment) & 14th amends.; *see Gitlow v. People of State of New York* (1925) 268 U.S. 652, 666 (First Amendment guarantees apply to the states through the due process clause of the Fourteenth Amendment).)
- 3) Provides that every person may freely speak, write, and publish their sentiments on all *subjects*, and that a law may not restrain or abridge liberty of speech. (Cal. Const., art. I, § 2 (Section 2).)

Existing state law:

- 1) Defines the following terms:

- a) "Digital replica" means 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; and does not include the electronic reproduction, use of a sample sound recording or audiovisual work into another, remixing, mastering, or digital remastering of a sound recording or audiovisual work authorized by the copyright holder. (Civ. Code, § 3344.1(a)(2)(B)(ii).)
 - b) "Generative artificial intelligence" means 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(a).)
 - c) "Large online platform" means a public-facing social media platform, file-sharing platform, mass-messaging platform, or standalone search engine that distributes content to users who did not create or collaborate in creating the content that exceeded 2,000,000 unique monthly users during the preceding 12 months, and does not include a broadband internet access service or a telecommunications service. (Bus. & Prof. Code, § 22757.1(h).)
 - d) "Covered material" means material that (1) is an image or video created or altered through digitization that would appear to a reasonable person to be an image or video of specified body parts or a person engaging in specified sexual acts; (2) the person did not consent to the use of their likeness in the material; and (3) the material is displayed, stored, or hosted on a social media platform. "Covered material" does not include an image or video that contains only minor alterations that do not lead to significant changes to the perceived content or meaning of the content, as specified. (Bus. & Prof. Code, § 22670(a).)
 - e) "Provenance data" means data that is embedded into digital content, or that is included in the digital content's metadata, for the purpose of verifying the digital content's authenticity, origin, or history of modification. (Bus. & Prof. Code, § 22757.1(o).)
- 2) Requires a social media platform, as defined, to provide a mechanism for a user to report sexually explicit identity theft, as defined, to the platform; to determine whether there is a reasonable basis to believe that the reported sexually explicit digital identity theft is sexually explicit digital identity theft; and, upon a determination that an image constitutes sexually explicit digital identity theft, to remove the image from being publicly viewable on the platform. (Bus. & Prof. Code, § 22671.)
 - 3) Provides that a preliminary injunction or temporary restraining order may be granted at any time before judgment in a civil action, as follows:

- a) A preliminary injunction may be granted at any time before judgment upon a verified complaint, or upon affidavits, if the complaint or affidavit shows satisfactorily that sufficient grounds exist for the injunction, except that no injunction may be granted without notice to the opposing party.
 - b) A temporary restraining order may be granted without notice to the opposing party if all of the following are satisfied:
 - i. It appears from the facts shown by affidavit or verified complaint that great or irreparable injury will result to the applicant before the matter can be heard on notice.
 - ii. The applicant or their attorney certifies, under oath, that they provided notice to the opposing party, or information as to why they were unable to or should not be required to provide such notice.
 - c) If the court issues a temporary restraining order without notice, the matter shall be made returnable on an order to show cause why a preliminary injunction should not be granted, on the earliest day possible for the court, but not later than 15 days, or 22 days for good cause, from the date the temporary restraining order is issued. (Code Civ. Proc., § 527.)
- 4) Provides causes of action for the dissemination of sexually explicit images, as specified, depicting an individual without their consent, as follows:
- a) For an image that actually depicts the individual, the individual has a private cause of action against a person who intentionally depicts the image if they knew or should have known that the other person had a reasonable expectation that the material would remain private, unless the individual waived any reasonable expectation of privacy in the image or the material constitutes a matter of public concern. (Civ. Code, § 1708.85.)
 - b) For a sexually explicit image that is a deepfake or an otherwise artificially altered image of the individual, but the individual is still identifiable, the depicted individual has a cause of action against a person who creates or disseminates the image, if that person knew or should have known that the individual did not consent to the image's creation or was a minor when the image was created. (Civ. Code, § 1708.86.)
- 5) 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 purposes of advertising or selling, or soliciting purchases of, products, merchandise, goods, or services, without that person's prior consent, shall be liable for actual damages and statutory damages, and may be liable for punitive damages. (Civ. Code, § 3344(a).)
- 6) Provides that a person who uses a deceased personality's name, voice, signature, photograph, or likeness, in any manner, including through the use of a digital replica, within 70 years after the death of the deceased personality, 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 from the person to whom the deceased personality transferred the rights, shall be liable for actual damages and statutory damages, and may be liable for punitive damages. (Civ. Code, § 3344.1.)

- 7) Provides that a court shall award attorney's fees and costs to the prevailing party in a suit under 4) or 5). (Civ. Code, §§ 3344(a), 3344.1(a).)
- 8) Provides that 4) and 5) do not apply to the owners or employees of any medium used for advertising, including, but not limited to, newspapers, magazines, radio and television networks and stations, cable television systems, billboards, and transit advertisements, by whom any violating advertisement or solicitation is published or disseminated, unless it is established that the owners or employees had knowledge of the unauthorized use of the deceased personality's name, voice, signature, photograph, or likeness as prohibited. (Civ. Code, §§ 3344(e), 3344.1(l).)

This bill:

- 1) Establishes the Digital Dignity Act.
- 2) Makes findings and declarations relating to the rapid and widespread availability of GenAI, the harms that can arise from unauthorized digital replicas, and the need for additional laws to prevent those harms.
- 3) Establishes a new Chapter within Division 8 of the Business and Professions Code, Chapter 8.
- 4) Defines the following terms within Chapter 8:
 - a) "Digital replica" has the same meaning as defined in Civil Code section 3344.1.
 - b) "Generative artificial intelligence" or "generative AI" has the same meaning as in Civil Code section 3110.
 - c) "Generative AI tool" means a generative AI system that is publicly accessible within the geographic boundaries of the state.
 - d) "Individual" means a natural person, whether living or deceased.
 - e) "Large online platform" has the same meaning as defined in Business and Professions Code section 22757.1.
 - f) "Nonconsensual intimate images" has the same meaning as "covered material" in Business and Professions Code section 22670.
 - g) "Provenance data" has the same meaning as defined in Business and Professions Code section 22757.1.
 - h) "Voice" means the actual or simulated sound of an individual's voice that is recognizable as the voice of that individual.

- 5) Requires the terms of service for any generative AI tool to explicitly prohibit users from creating content that violates the Digital Dignity Act, including the creation of nonconsensual intimate images.
- 6) Requires a generative AI tool provider to maintain, for no fewer than 90 days, records sufficient to allow compliance with a court order issued pursuant to 14), including records identifying any provenance data associated with a digital replica, if the records do not include the content of user communications.
- 7) Requires a product, service, website, or application that is both a generative AI tool and a large online platform that allows users to create a digital replica of other individuals to implement and maintain a mechanism by which users can do both of the following:
 - a) Revoke access to their digital replica.
 - b) Remove any photograph, video, audio recording, or other digital rendering that includes their digital replica created by other people using the large online platform's generative AI tool at any time.
- 8) Requires a platform in 7) to allow users to remove videos containing their digital replica created by other people using the large online platform's generative AI tool at any time.
- 9) Provides that 7) and 8) do not require the covered platform to provide access to content that is generated and stored exclusively on a user's local device and that has not been transmitted to the product's, service's, website's, or application's servers.
- 10) Requires a large online platform to provide a clear, conspicuous, and easy-to-use mechanism for a user to report a digital replica that violates the Digital Dignity Act, regardless of whether or not the individual depicted is a user of the generative AI tool or large online platform.
- 11) Requires a large online platform, to prevent unfair or deceptive acts or practices in the administration of the reporting mechanisms required by 10), to maintain a reporting process that ensures within 48 hours of receiving a user report all of the following occurs:
 - a) Reports of unauthorized digital replicas are reviewed.
 - b) If the content violates the Digital Dignity Act, access to the content is removed or disabled.
 - c) The reporting party is provided with a confirmation of the removal or, if the content was not removed, a written explanation of the reason.
- 12) Provides that a platform's systematic failure to adhere to the timelines and to process valid reports in good faith constitutes a violation of Chapter 8.

- 13) Provides that a city attorney or the Attorney General may bring a civil action to enforce Chapter 8 and may seek a civil penalty not to exceed \$50,000 for each day a generative AI tool is provided to the public in violation of Chapter 8.
- 14) Provides that a city attorney or the Attorney General may seek an injunction or temporary restraining order prior to the judgment pursuant to Code of Civil Procedure section 527; if the court grants the applicant a temporary restraining order that requires the respondent to remove, recall, or otherwise cease publication or distribution of the petitioner's name, voice, signature, photograph, or likeness, the respondent shall complete the removal or recall, or cease the publication or distribution, within two business days from the day the order is served, unless otherwise required by the order.
- 15) Adds a new section to the Civil Code, Section 3344.2, set forth in 16).
- 16) Provides that any person that, by distributing content with actual knowledge that the content includes the use of a digital replica, is found liable in a civil action for defamation or violates a provision of the Penal Code in which false impersonation of another is a required element, including, without limitation, Penal Code sections 528.5, 529, and 630, shall also be liable for the greater of the following:
 - a) If an individual or entity negligently distributes, liquidated damages of \$1,000 or actual damages for each violation.
 - b) If a violation was committed by an individual or entity with knowledge of, or reckless disregard for, the rights of the individual, the court may, in its discretion, award not less than \$5,000 for each violation.
- 17) Provides that, in addition to the remedies available in 16), a party may seek an injunction or temporary restraining order pursuant to Code of Civil Procedure section 527; if the court grants the applicant a temporary restraining order that requires the respondent to remove, recall, or otherwise cease publication or distribution of the petitioner's name, voice, signature, photograph, or likeness, the respondent shall complete the removal or recall, or cease the publication or distribution, within two business days from the day the order is served, unless otherwise required by the order.
- 18) Provides that the rights in 16) shall apply until 70 years after the year of the imitated person's death.
- 19) Provides that the rights recognized under 15) are property rights, freely transferrable or descendible, in whole or in part, by contract, by means of trust, or by existing statute.
- 20) Provides that 15) shall not be construed to render invalid or unenforceable a contract entered into by a living person that assigned the rights, in whole or in part, to the living person's name, voice, signature, photograph, or likeness.

- 21) Provides that, for purposes of 15), a digital replica may be used without consent if the digital replica meets the conditions of existing exceptions within Civil Code section 3344.1, as follows:
- a) The use of a name, voice, signature, photograph, or likeness is in connection with any news, public affairs, or sports broadcast or account, or any political campaign.
 - b) The use of a digital replica meets any of the following criteria:
 - i. The use is in connection with any news, public affairs, or sports broadcast or account.
 - ii. The use is for purposes of comment, criticism, scholarship, satire, or parody.
 - iii. The use is a representation of the individual as the individual's self in a documentary or in a historical or biographical manner, including some degree of fictionalization, unless the use is intended to create, and does create, the false impression that the work is an authentic recording in which the individual participated.
 - iv. The use is fleeting or incidental.
 - v. The use is in an advertisement or commercial announcement for a work described in (i)-(iv).
- 22) Provides that 15) shall apply to the adjudication of liability and the imposition of any damages or other remedies in cases in which the liability, damages, and other remedies arise from acts occurring directly in this state.
- 23) Provides that the remedies provided for in 15) are cumulative and shall be in addition to any others provided for by law.
- 24) Provides that nothing in 15) shall be construed to conflict with or preempt federal law or regulation, and that 15) does not impose liability on a social media platform if that liability is prohibited by Section 230 of Title 47 of the United States Code.
- 25) Includes a severability clause.

COMMENTS

1. Author's comment

According to the author:

With rapid improvements in AI image, video, and audio generation, highly realistic computer-generated depictions of people's voice and likeness have become increasingly common across large online platforms. The widespread availability of these AI tools has enabled bad actors to create Digital Replicas of individuals that may be used to harm their personal reputation, social standing,

employment status, as well as their physical and emotional well-being. Generative AI tools have been used to create non-consensual intimate imagery, to perpetrate financial fraud against individuals and businesses, to create false endorsements, to defame and harass individuals, and to deceive the public through fraudulent impersonation. Early in 2024, an employee at UK engineering company, Arup, was tricked into transferring over \$25 million after attending a video conference call where every other participant, including the “CFO” was a deepfake. More recently, in early 2026, users exploited features in xAI’s Grok model to generate and circulate non-consensual sexual images of real people, leading to regulatory investigations. And in 2026, employment fraud spiked as operatives from North Korea used real-time deepfake video and audio to pass remote job interviews at U.S. companies to infiltrate sensitive systems. These examples are only a few instances, in a rising tide of deceptive practices, that highlight the need for urgent action.

Current defamation law does not account for the particularly egregious harm that the use of digital replicas to defame others inflicts. Additionally, the integration of GenAI tools with large online platforms calls for additional obligations on such platforms to provide users with more control over the use of their likeness as it relates to those tools specifically. SB 1142 seeks to address these concerns by providing additional specified damages for those found liable for defamation and false impersonation using a digital replica. Additionally, the bill imposes reasonable and technically feasible obligations on large online platforms who provide GenAI tools users can use to create digital replicas of themselves and others. Together, these solutions would ensure Californians have meaningful control over their likeness online, and impose real consequences on those who seek to weaponize this technology to defame or impersonate them.

2. Background on one’s rights to one own image

As a general rule, a person isn’t legally entitled to control or limit the use of their own image by others. When an artist captures a person’s image in a “tangible medium of expression,” such as a photograph or film, the Copyright Act of 1976 gives the rights to that work to the artist, not the subject.¹ The Copyright Act expressly preempts any state laws that are “equivalent to any of the exclusive rights within the general scope of copyright” covered by the Act.²

Courts recognize, however, that the Copyright Act’s preemption clause leaves intact certain state laws relating to the unauthorized use of one’s image. These state laws, which generally create civil causes of action for the unauthorized use, arise out of circumstances where the person featured in the work is harmed because of the *nature* of how they are portrayed, not the mere fact of their portrayal. These claims include the

¹ See 17 U.S.C. § 102.

² *Id.*, § 301.

right of publicity; defamation and the tort of false light invasion of privacy; and the state's various provisions relating to nonconsensual sexual imagery, whether real or artificially generated.³

The right of publicity, which is both a common law right and a statutory one, arises when a person uses the identity of another for their own advantage without the subject's consent; the statutory claim also requires that the unauthorized use be for a commercial purpose.⁴ The injury in a right of publicity action arises not from the unauthorized use as such, but from the defendant's misappropriation of the economic value generated by the plaintiff's (often hard-won) popularity and reputation.⁵ California also has a statutory postmortem right of publicity, which prohibits the use of a deceased person's name, voice, signature, photograph or likeness, on or in products, or for purposes of advertising, without the consent of the deceased person's heir or person holding the publicity right, for 70 years following the person's death.⁶ Both the statutory right of publicity and postmortem right of publicity explicitly extend to the use of digital replicas.⁷

The tort of defamation from "the intentional publication of a statement which is false, unprivileged, and has the natural tendency to injure or which causes special damage."⁸ California also has a related common-law tort known as "false light invasion of privacy," which protects an individual from "publicity that places [an individual] before the public in a false light that would be highly offensive to a reasonable person, and where the [publisher] knew or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the [individual] would be placed."⁹ These torts are both "reputational": a person can experience severe harm from being portrayed in an offensive, but false, manner, and should be able to recover from the individual who knowingly published the misleading portrayal.¹⁰

Recently, the state has added protections against the dissemination of sexually explicit materials published without the consent of a person depicted in the image. These

³ California also criminalizes various forms of impersonation of another where, e.g., the impersonation is for purposes of harming, harassing, intimidating, threatening, or defrauding another, or for the purpose of obtaining a benefit or property to which they are not entitled. (See, e.g., Pen. Code, §§ 528.5, 529, 530.) As criminal statutes, these violations cannot be vindicated by the person whose identity was misused, though in many cases the criminal violation could also give rise to civil liability under existing law.

⁴ See *Downing v. Abercrombie & Fitch* (9th Cir. 2001) 265 F.3d 994, 1001. The right of publicity statute specifies that the unauthorized use of a plaintiff's name, voice, signature, photograph, or likeness for commercial gain are all prohibited. (Civ. Code, § 3344.)

⁵ *Timed Out, LLC v. Youabian, Inc.* (2014) 229 Cal.App.4th 1001.

⁶ Civ. Code, § 3344.1.

⁷ See *id.*, § 3344, 3344.1

⁸ *Gilbert v. Sykes* (2007) 147 Cal.App.4th 13, 27 (internal quotation marks omitted); see Civ. Code, §§ 44-47.

⁹ *DeHavilland v. FX Networks, LLC* (2018) 21 Cal.App.5th 845, 865 (internal quotation marks omitted).

¹⁰ See *Fellows v. National Enquirer, Inc.* (1986) 42 Cal.3d 234, 239 ("Although it is not necessary that the plaintiff be defamed, publicity placing one in a highly offensive light will in most cases be defamatory as well").

protections apply in cases where the image actually depicts the individual, but the individual consented to the creation of the image with a reasonable expectation that the image would stay private (e.g., revenge porn), as well as in cases of “deepfake” pornography created without the individual’s consent.¹¹ Similarly, in 2025, the federal government enacted the TAKE IT DOWN Act, which requires a social media platform to remove sexually explicit imagery upon request from a person depicted in the image who did not consent to the image’s dissemination.¹²

The Copyright Office reported in 2025 that the existing federal and state legal framework is insufficient to adequately protect individuals from the misuse of their digital replicas.¹³ The Copyright Office noted that state laws relating to the unauthorized use of one’s image “are both inconsistent and insufficient in various respects,”¹⁴ while “[e]xisting federal laws are too narrowly drawn to fully address harm from today’s sophisticated digital replicas.”¹⁵ These harms are discussed in Comment 3, below.

3. GenAI image generation: release the tools first, add guardrails later (or not at all)

As explained by the Senate Privacy, Digital Technologies, and Consumer Protection Committee’s analysis of this bill:

The world has been in awe of the powers of generative AI since the widespread introduction of AI systems such as ChatGPT. However, the capabilities of these advanced systems lead to a blurring between reality and fiction. The rapid advancement of AI technology has created unprecedented challenges in protecting individuals’ identities and likenesses. Deepfakes and AI-generated content can now convincingly mimic a person’s voice, appearance, and mannerisms, making impersonation easier and more convincing than ever before. The Brookings Institution lays out the issue:

Over the last year, generative AI tools have made the jump from research prototype to commercial product. Generative AI models like OpenAI’s ChatGPT and Google’s Gemini can now generate realistic text and images that are often indistinguishable from human-authored content, with generative AI for audio and video not far behind. Given these advances, it’s no longer surprising to see AI-generated images of public figures go viral or AI-generated reviews and comments on digital platforms. As

¹¹ See Civ. Code, §§ 1708.85, 1708.86.

¹² 47 U.S.C. § 223a.

¹³ United States Copyright Office, Copyright and Artificial Intelligence, Part 1: Digital Replicas (Jan. 2025) pp. 23-24, available at <https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-1-Digital-Replicas-Report.pdf>. All links in this analysis are current as of April 16, 2026.

¹⁴ *Id.* at p. 23.

¹⁵ *Id.* at p. 24.

such, generative AI models are raising concerns about the credibility of digital content and the ease of producing harmful content going forward.

Against the backdrop of such technological advances, civil society and policymakers have taken increasing interest in ways to distinguish AI-generated content from human-authored content.¹⁶

More recently, advanced tools like OpenAI's (recently discontinued) Sora and xAI's Grok have captured the public's attention with highly realistic digital replicas of actual persons in images and videos. However, this has brought with it troubling instances of nonconsensual uses of others' likenesses:

Elon Musk's artificial intelligence chatbot, Grok, created and then publicly shared at least 1.8 million sexualized images of women, according to separate estimates of X data by The New York Times and the Center for Countering Digital Hate.

Starting in late December, users on the social media platform inundated the chatbot's X account with requests to alter real photos of women and children to remove their clothes, put them in bikinis and pose them in sexual positions, prompting a global outcry from victims and regulators.

In just nine days, Grok posted more than 4.4 million images. A review by The Times conservatively estimated that at least 41 percent of posts, or 1.8 million, most likely contained sexualized imagery of women. A broader analysis by the Center for Countering Digital Hate, using a statistical model, estimated that 65 percent, or just over three million, contained sexualized imagery of men, women or children.

The findings show how quickly Grok spread disturbing images, which earlier prompted governments in Britain, India, Malaysia and the United States to start investigations into whether the images violated local laws. The burst of nonconsensual images in just a few days surpassed collections of sexualized deepfakes, or realistic A.I.-generated images, from other websites, according to The Times's analysis and experts on online harassment.¹⁷

¹⁶ Srinivasan, *Detecting AI fingerprints: A guide to watermarking and beyond* (January 4, 2024) Brookings Institution, <https://www.brookings.edu/articles/detecting-ai-fingerprints-a-guide-to-watermarking-and-beyond/>.

¹⁷ Conger, Freedman, & Thompson, *Musk's Chatbot Flooded X With Millions of Sexualized Images in Days, New Estimates Show* (Jan. 22, 2026) New York Times, <https://www.nytimes.com/2026/01/22/technology/grok-x-ai-elon-musk-deepfakes.html>.

This has led to a number of lawsuits and actions by the California Attorney General Rob Bonta.¹⁸

4. This bill establishes the Digital Dignity Act to give a person control over their digital replica created by generative AI on a large online platform

This bill establishes the Digital Dignity Act and provides two mechanisms to prevent, or penalize, the unauthorized use of a person's digital replica.

First, the bill requires a product, service, website, or application that is both a generative AI tool and a large online platform that allows users to create a digital replica of other individuals to implement and maintain a mechanism allowing users to (1) revoke access to their digital replica and (2) remove content that includes their digital replica created by other people using the generative AI tool. Users must be permitted to remove, at any time, videos containing their digital replica using that generative AI tool, as provided. A covered platform is also required to provide a mechanism for users to report digital replicas that violate this Act and to respond to takedown requests within 48 hours, as provided. A covered platform is required to explicitly prohibit the creation of content that violates these provisions within their terms of service. A platform's systemic failure to adhere to the timelines and process requirements in good faith constitutes a violation of the Act. As discussed further in Comment 5, below, the bill currently raises concerns that it will overly constrain protected speech; the author has agreed to amendments to address this issue, set forth in Comment 6, below.

The Attorney General or a city attorney may bring a civil action to enforce the provisions set forth above. The bill requires a covered platform to maintain specified records for at least 90 days to facilitate compliance with court orders arising from such an action. The bill provides for a civil penalty of up to \$50,000 per day that the platform is in violation of the Act and permits the Attorney General or city attorney to seek injunctive relief, including prior to the entry of judgment.

Second, the bill provides for enhanced remedies for the unauthorized use of a person's digital replica in certain contexts. The enhanced remedy is against a person who, by distributing content with actual knowledge that the content includes the use of a digital replica:

- Is found liable in a civil action for defamation; or
- Violates a provision of the Penal Code in which false impersonation of another is a required element, including the crimes of credible impersonation of an action

¹⁸ Johnson, *California orders Elon Musk's AI company to immediately stop sharing sexual deepfakes* (Jan. 14, 2026) CalMatters, <https://calmatters.org/economy/technology/2026/01/california-investigates-deepfakes-elon-musk-company/>; Padilla, *Teens sue Musk's xAI, arguing Grok made child sexual abuse material* (Mar. 16, 2026) USA Today, <https://www.usatoday.com/story/news/california/2026/03/16/elon-musk-xai-faces-class-action-lawsuit-over-ai-generated-deepfakes-grok-teens-child-images-sexual/89144313007/>.

person on a website or other electronic means and false impersonation of another in a private or official capacity.¹⁹

The author has agreed to amendments to apply this enhanced remedy consistently across misappropriation-of-image torts, to clarify that all relevant defenses to such torts will continue to apply, and to make other clarifying changes.

5. Constitutional issues

a. First Amendment questions

For purposes of a First Amendment analysis, a law is considered “content based if a law applies to particular speech of the topic discussed or message expressed.”²⁰ When a state law imposes a content-based restriction on speech, a First Amendment challenge will subject the law to “strict scrutiny.”²¹ “To satisfy strict scrutiny, a restriction on speech is justified only if the government demonstrates that it is narrowly tailored to serve a compelling state interest.”²²

Here, there is no question that the bill addresses a compelling state interest: protecting individuals from defamatory, invasive, or humiliating images of themselves that may be indistinguishable from an actual photo or video. There is also no question that, in many cases, an unauthorized use of another’s digital replica could fall outside the First Amendment’s protections. For example, as the author notes, Grok, xAI’s chatbot and image generator, generates nonconsensual sexual imagery and child sexual assault material of women and girls;²³ of course the state has a compelling interest in protecting its residents from such violations.

It does appear, however, that this bill could be overbroad because it is likely to restrict constitutionally protected speech. Although this is a relatively novel area of law, a recent legal challenge to AB 2655,²⁴ California’s prohibition on deepfake videos in elections, may serve as a guide here.²⁵ In that case, the district court recognized that California has a compelling interest in protecting free elections, but still enjoined

¹⁹ See Pen. Code, §§ 528.5, 529, 530.

²⁰ *Reed v. Town of Gilbert, Ariz.* (2015) 576 U.S. 155, 163.

²¹ *Id.* at pp. 163-164.

²² *Twitter, Inc. v. Garland* (9th Cir. 2023) 61 F.4th 686, 698.

²³ E.g., Gentleman & Horton, ‘Add blood, forced smile’: how Grok’s nudification tool went viral (Jan. 11, 2026) *The Guardian*, <https://www.theguardian.com/news/ng-interactive/2026/jan/11/how-grok-nudification-tool-went-viral-x-elon-musk>; Vincens & Satter, *Elon Musk’s Grok AI floods X with sexualized photos of women and minors* (Jan. 3, 2026; updated Jan. 4, 2026) *Reuters*, <https://www.reuters.com/legal/litigation/grok-says-safeguard-lapses-led-images-minors-minimal-clothing-x-2026-01-02/>.

²⁴ Berman, Ch. 261, Stats. 2024.

²⁵ See *Kohls v. Bonta* (E.D. Cal. 2025) 797 F.Supp.3d 1177, 1183. The law in question had an exemption for parody and satire, but required the content creator to include a disclaimer stating that the content had been manipulated for purposes of satire or parody. (See Elec. Code, § 20012.)

AB 2655 because it was not narrowly tailored: it prohibited more speech than those categories which fall outside First Amendment protection.²⁶

In order to address the potential First Amendment issues raised by this bill, the author has agreed to amend the bill as set forth in Comment 6, below.

b. Section 230

Opponents of the bill argue that the takedown mechanism and liability for a platform that fails to take down an unauthorized digital replica violate Section 230 of the Communications Decency Act.²⁷ Section 230 has two main components. The first provides that “[n]o 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.”²⁸ The second provides a safe harbor for content moderation, by stating that no provider or user shall be held liable because of good-faith efforts to restrict access to material that is “obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected.”²⁹ Together, these two provisions give platforms immunity from any civil or criminal liability that could be incurred by user statements, while explicitly authorizing platforms to engage in their own content moderation without risking that immunity.

This bill addresses content generated by, and posted on, the platform’s own generative AI tool. Although no court has specifically addressed the issue, it does not appear that such content qualifies as content generated by “another information content provider” for purposes of Section 230 protections.

6. Amendments

As discussed above, the author has agreed to amend as set forth below, subject to any nonsubstantive changes the Office of Legislative Counsel may make.

Amendment 1

On page 2, in lines 21-22, delete “control the use of their own identity” and insert “protect against the misappropriation of their likeness”

Amendment 2

On page 3, in line 32, after “is” insert “capable of creating digital replicas and”

²⁶ *Kohls, supra*, 797 F.Supp.3d at pp. 1185, 1186-1187. The Attorney General has appealed this case to the Ninth Circuit and briefing is ongoing.

²⁷ See 47 U.S.C. § 230.

²⁸ *Id.*, § 230(c)(1).

²⁹ *Id.*, § 230(c)(1) & (2).

Amendment 3

On page 4, in line 14, after “images.” insert “A provider satisfies this requirement if its terms of service contain a general prohibition on the creation of unauthorized digital replicas or the unlawful use of an individual’s likeness.”

Amendment 4

On page 4, delete lines 21-40, and at page 5, delete lines 1-21, and insert:

(c) A large online platform that includes a generative AI tool that provides users with the functionality to create a digital replica of other individuals shall provide a clear, conspicuous, and easy-to-use reporting mechanism for an individual, whether or not they are a user of the large online platform, to do all of the following:

(1) (A) Report content that violates the platform’s terms of service or a provision of law relating to the individual’s digital replica.

(B) A process established pursuant to Section 223a of Title 47 of the United States Code shall satisfy the requirement of this paragraph, provided that the process allows an individual to report any violation of the terms of service or provision of law.

(2) (A) Submit to the large online platform any certified court order or judgment, including an injunction awarded pursuant to Section 527 of the Code of Civil Procedure, ordering the removal of any content involving the individual’s digital replica on the platform or finding that content involving the individual’s digital replica was defamatory, fraudulent, or any other form of image appropriation not permitted by law.

(B) Upon receipt of a court order or judgment under this paragraph, the large online platform shall, as soon as possible, but not later than 48 hours after receiving such the court order or judgment, remove the intimate visual depiction and make reasonable efforts to identify and remove any known identical copies of such depiction.

Amendment 5

On page 5, in line 33, delete “name, voice, signature, photograph, or likeness” and insert “digital replica”

Amendment 6

On page 5, delete lines 38-40, and on page 6, delete lines 1-4, and insert:

3344.2. (a) Any person that, by distributing content with actual knowledge that the content includes a digital replica, is found liable in a civil action arising from the use or portrayal of that digital replica or is found guilty of violating a provision of the Penal Code for which false impersonation of another is a required element, including, without limitation, Sections 528.5, 529, and 530 of the Penal Code, shall also be liable for the greater of the following:

Amendment 7

On page 6, in line 18, delete “name, voice, signature, photograph, or likeness” and insert “digital replica”

Amendment 8

On page 6, delete lines 22-23.

Amendment 9

On page 6, delete line 31 and line 32 through “if” and insert “This section shall not be construed to affect or limit any defenses available in the underlying civil or criminal action, including, but not limited to, that”

7. Arguments in support

According to the Transparency Coalition:

With rapid improvements in AI image, video, and audio generation, highly realistic computer-generated depictions of people’s voice and likeness have become increasingly common across large online platforms. The widespread availability of these AI tools has enabled bad actors to create Digital Replicas of individuals that may be used to harm their personal reputation, social standing, employment status, as well as their physical and emotional well-being. Generative AI tools have been used to create non-consensual intimate imagery, to perpetrate financial fraud against individuals and businesses, to create false endorsements, to defame and harass individuals, and to deceive the public through fraudulent impersonation.

Current law does not account for the particularly egregious harm that the use of digital replicas to defame others inflicts. Additionally, the integration of GenAI tools with large online platforms calls for additional obligations on such platforms to provide users with more control over the use of their likeness as it relates to those tools specifically.

Dignity-based protections recognize the intrinsic worth of human beings shared by all people, as well as the individual reputation of each person built upon their own

individual actions and achievements. Violations of dignity-based protections, unlike property right violations, do not manifest in clear monetary or financial losses. Instead, violations of one's dignity produce emotional harms like distress, embarrassment, or humiliation, as well as psychological harms. Violations may also cause reputational harm, including being misrepresented in relation to a matter, including one's beliefs, identities, and actions, and/or experiencing disadvantageous changes in employment status, position, or duties as a result of the violation. Monetary and financial harms can accompany dignity-based violations, including resultant damage to property or damage to a business or financial position.

SB 1142 seeks to address these concerns by providing additional specified damages for those found liable for defamation and false impersonation using a digital replica. Additionally, the bill imposes reasonable and technically feasible obligations on large online platforms who provide GenAI tools users can use to create digital replicas of themselves and others. Together, these solutions would ensure Californians have meaningful control over their likeness online and impose real consequences on those who seek to weaponize this technology to defame or impersonate them.

8. Arguments in opposition

According to a coalition of the bill's opponents:

The notice-and-takedown framework proposed in SB 1142 raises significant constitutional concerns by bypassing judicial oversight in favor of a private reporting system. Under the First Amendment, the government generally cannot compel the removal of speech without a prior judicial determination that the content is legally unprotected. By requiring covered platforms to act on individual reports of "unauthorized digital replicas" without a court first adjudicating whether a violation has actually occurred, the bill essentially delegates a quasi-judicial function to private entities. This lack of due process risks suppressing constitutionally protected content, such as political parody or news reporting, before it can ever be evaluated by an impartial judge.

Furthermore, the bill's structure creates an inevitable chilling effect on legitimate expression. Because SB 1142 holds "large online platforms" liable for failing to act once they have "actual knowledge" of a violation, platforms are financially incentivized to adopt a 'remove-first' policy. To mitigate the risk of costly litigation and statutory damages, they will likely over-remove any flagged content that sits in a legal gray area. Some expressions that may depict an individual could be First Amendment-protected content such as satire, commentary, or transformative art. In such an environment, the mere threat of a report can effectively censor a speaker, leading to the systemic disappearance of lawful discourse.

SUPPORT

Transparency Coalition (sponsor)
California Institute for Technology & Democracy
California Orthopaedic Association
California Podiatric Medical Association
California Society of Pathologists
CFT – A Union of Educators & Classified Professionals, AFT, AFL-CIO
Kapor Center Advocacy
Music Artists Coalition

OPPOSITION

California Chamber of Commerce
Civil Justice Association of California
Computer & Communications Industry Association
Internet Works
Motion Picture Association
Oakland Privacy
TechNet

RELATED LEGISLATION

Pending legislation:

SB 1146 (Gonzalez, 2026) requires ads for health products, as defined, that include an AI-generated digital replica or synthetic performer purporting to be a licensed medical professional to include specified disclosures. SB 1146 is pending before the Senate Appropriations Committee.

SB 1111 (Ashby, 2026) clarifies that, within California’s right of publicity statute, a voice or likeness includes a digital replica, as defined. SB 1111 is pending before the Senate Public Safety Committee.

Prior legislation:

SB 11 (Ashby, 2025) would have ensured that computer-manipulated or generated content is incorporated into the right of publicity law and criminal false impersonation statutes by requiring that those making available such technology to provide a warning to consumers about liability for misuse, as provided. This bill also would have required the Judicial Council to review the impact of AI on evidence introduced in court proceedings and to adopt rules of court as necessary. Governor Newsom vetoed the bill, stating in his veto message that “it is unclear whether a warning would be sufficient to dissuade wrongdoers from using AI to impersonate others without their consent.”

AB 853 (Wicks, Ch. 674, Stats. 2025) established requirements on large online platforms, capture device manufacturers, and GenAI system hosting platforms to embed and disclose provenance data in content generated or altered by GenAI systems, as provided, with the requirements to take effect on January 1, 2027.

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

SB 942 (Becker, Ch. 291, Stats. 2024) required businesses that provide generative AI systems to make accessible tools to detect whether specified content was generated by those systems; these “covered providers” are required to offer visible, and include imperceptible, markings on AI-generated content to identify it as such.

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

PRIOR VOTES:

Senate Privacy, Digital Technologies, and Consumer Protection Committee (Ayes 7,
Noes 0)
