SENATE THIRD READING
SB 11 (Ashby)
As Amended
Majority vote

SUMMARY

Requires sellers of AI tools that enable a user to create digital replicas to provide a consumer warning about potential legal liability for unlawful use, clarifies that realistic digital replicas may violate a person′s right of publicity, directs the Judicial Council to address AI-generated evidence in court proceedings, and clarifies that the use of a digital replica to impersonate another qualifies as ″false impersonation.″

Major Provisions

1) Requires, by December 1, 2026, a person or entity that sells or provides access to any AI technology that enables a user to create a digital replica to provide a consumer warning that unlawful use of the technology may result in civil or criminal liability for the user.

2) Subjects violators to a civil penalty not to exceed $25,000 for each day that the technology is provided to or offered to the public without a consumer warning in a civil action brought by a public prosecutor.

3) Provides, for purposes of the right of publicity law, that a voice or likeness includes a digital replica.

4) Removes the rebuttable presumption from the right of publicity statute.

5) Requires, by no later than 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.

6) Defines the following terms:

   a) ″Artificial intelligence″ has the same meaning as in Section 3110 of the Civil Code.

   b) ″Digital replica″ has the same meaning as in Section 3344.1 of the Civil Code.

7) Provides that for the purposes of all Penal Code provisions for which the false impersonation of another is a required element, including, without limitation, Sections 528.5, 529, and 530, false impersonation includes the use of a digital replica with the intent to impersonate another.

COMMENTS

The rapid proliferation of generative artificial intelligence (GAI) has transformed the creation and dissemination of digital content. GAI systems such as OpenAI′s ChatGPT, Google′s Gemini, and Anthropic′s Claude use neural networks trained on vast datasets to generate highly realistic text, audio, images, and video that closely resemble human-authored content. These tools allow

users to create synthetic media via simple text prompts and are widely available at low or no cost. As a result, virtually anyone can produce lifelike digital representations of real individuals—living or deceased—without consent or disclosure.

While GAI offers substantial benefits for education, creative expression, and productivity, it also introduces acute risks to personal autonomy, public trust, and democratic institutions. The realism of AI-generated content increasingly renders it indistinguishable from authentic content. This ″blurring of reality″ facilitates impersonation, fraud, false endorsements, political disinformation, and reputational attacks. Synthetic media can depict an individual engaged in criminal or sexual conduct or appearing to incite violence or confess to crimes—without that person′s knowledge or participation. (*See* Chesney & Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security* (2019) 107 Cal. L. Rev. 1753, 1756–1759.)

These concerns extend to evidentiary settings. Courts are already confronting questions about whether digital images, video, or audio offered as evidence have been manipulated using AI. As the public becomes more aware of AI′s ability to fabricate media, bad actors may falsely claim that authentic evidence is synthetic—a tactic known as the ″liar′s dividend.″ (*Id.*) This phenomenon poses serious threats to truth-seeking in court, journalism, and public discourse.

Although emerging techniques like watermarking, content provenance, and detection models offer partial safeguards, none are foolproof and all require continuous updating to remain effective. (*See* Srinivasan, *Detecting AI Fingerprints: A Guide to Watermarking and Beyond* (Jan. 4, 2024) Brookings Institute, https://www.brookings.edu/articles/detecting-ai-fingerprints-a-guide-to-watermarking-and-beyond.) Experts have urged judicial rulemakers to adopt evidentiary standards and develop tools for authenticating digital media. (*See* Zoppo, *Threat of AI-Generated 'Deepfake' Evidence Needs Judiciary's Attention, Former Judge Says* (Oct. 27, 2023) National Law Journal, https://www.law.com/nationallawjournal/2023/10/27/threat-of-ai-generated-deepfake-evidence-needs-judiciarys-attention-former-judge-says.)

SB 11 attempts to address these problems by clarifying that synthetic content can constitute false impersonation under existing Penal Code provisions, expanding publicity rights under Civil Code Section 3344 to AI-generated likenesses, requiring consumer warnings from sellers of AI tools capable of generating digital replicas, and directing the Judicial Council to develop rules of court to assist trial courts in evaluating evidence believed to be AI-generated.

This bill is substantially similar to SB 970 (Ashby, 2024), which was held in Senate Appropriations Committee last session.

*Consumer warnings***.** This bill requires any person or entity that sells, offers, or otherwise provides access to a tool that enables a user to create digital replicas to display a consumer warning. This warning must inform users that misuse of the technology may subject them to civil or criminal liability. Sellers of such tools must begin providing this warning to users by December 1, 2026. Failure to comply may result in civil penalties of up to $25,000 per day. This provision reflects a growing consensus that downstream users of generative AI tools—many of whom may not fully understand the legal implications of their use—should be affirmatively notified of the risks associated with creating realistic synthetic media.

California law has long required consumer-facing legal exposure disclosures in contexts where individuals might unknowingly engage in conduct subject to liability. Examples include

warnings on cannabis packaging (Business and Professions Code Section 26120) and firearm transfers (Penal Code Section 26835). SB 11 follows this tradition by ensuring that users are made aware that digital impersonation using AI-generated content could violate existing laws, including statutes prohibiting false impersonation, deepfake pornography, and the unauthorized use of likeness.

Digital replicas. SB 11 amends California′s right of publicity statute for living individuals—Civil Code Section 3344—to clarify that a digital replica of a person′s voice or likeness that is readily identifiable as the voice or visual likeness of that individual shall be treated as the actual voice or likeness of that person under the statute. This clarification ensures that highly realistic AI-generated simulations cannot evade liability under Section 3344 simply because they were created synthetically rather than derived from preexisting recordings or images. The bill thus updates the statutory framework to reflect technological developments that allow AI tools to produce convincingly lifelike depictions of real people, often without their knowledge or consent. Structurally, this amendment parallels the approach taken in AB 1836 (Bauer-Kahan, Chap. 258, Stats. 2024), which similarly clarified liability for unauthorized digital replicas—though in that case, under Civil Code Section 3344.1, which governs postmortem publicity rights. SB 11′s amendment serves to modernize the legal understanding of ″likeness″ and ″voice″ to include hyper-realistic digital fabrications, closing a potential loophole in the state′s publicity rights framework.

Rebuttable presumption. SB 11 eliminates a provision from the original 1971 statute that created 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.

Judicial Council study on AI-generated evidence. The rise of generative artificial intelligence (AI) has created profound challenges for courts evaluating the admissibility, authenticity, and reliability of evidence. As increasingly realistic synthetic content—including deepfakes, AI-generated voice clones, and fabricated images—enters the courtroom, judges must grapple with whether existing evidentiary standards are sufficient to safeguard due process, jury integrity, and the adversarial process. Courts assess the admissibility of any proffered evidence through a framework grounded in the California Evidence Code, case law, and relevant Rules of Court. When any piece of evidence is proffered, courts conduct an analysis to determine its admissibility. Evidence must be relevant (Evidence Code Sections 210, 350), its probative value must not be substantially outweighed by prejudice or risk of misleading the jury (Section 352), and it must be authenticated before being admitted (Sections 1400–1402). In cases involving technical processes or data interpretation, expert testimony is generally required under Section 801 to authenticate the evidence, and must rest on reliable, scientifically valid methodology.

However, these traditional frameworks were not designed to address the unique evidentiary issues posed by generative AI. AI systems—particularly those based on machine learning and neural networks—often operate as ″black boxes″ whose internal logic may be opaque even to their developers. This lack of transparency complicates authentication, challenges expert qualifications, and undermines the fact-finder′s ability to assess credibility and weight. Scholars have described this as the ″inscrutability problem,″ where AI-generated results cannot be meaningfully explained or cross-examined.

Confrontation Clause jurisprudence also raises constitutional constraints. The U.S. Supreme Court has held that the Sixth Amendment requires a criminal defendant to have an opportunity to cross-examine witnesses who provide testimonial evidence. (*Crawford v. Washington* (2004) 541 U.S. 36, 68.) Courts are now debating whether outputs from AI models—particularly those generated outside of adversarial control—constitute testimonial hearsay, and if so, whether a human operator can meaningfully stand in as a surrogate witness. 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.

False impersonation. SB 11 amends California′s Penal Code to ensure that existing false impersonation statutes remain effective in the age of generative artificial intelligence. A wide range of California laws already prohibit false impersonation—defined as the unauthorized use of another′s name, image, or identity to cause harm or gain a benefit—including impersonation by electronic means (Penal Code Section 528.5) or to obtain money or property (Penal Code Section 530). However, these statutes were enacted in an era before the widespread availability of AI tools capable of generating synthetic voice and image content. To close this gap, SB 11 provides that for any criminal offense requiring false impersonation as an element, the use of a digital replica with the intent to impersonate another constitutes false impersonation.

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.

Arguments in Support

Common Sense Media explains its support of this measure:

> 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.

We support SB 11 as a necessary step toward addressing the growing threat of AI-enabled exploitation and abuse. As a leading advocate for safe and responsible technology, Common Sense Media has consistently pushed for stronger transparency, safety, and accountability in the development and deployment of artificial intelligence. As strong supporters of the recently enacted, bipartisan federal TAKE IT DOWN Act, we are committed to curbing the spread of non-consensual deep fakes and protecting those most at risk of digital harm. SB 11 furthers this effort by ensuring legal recourse for victims and requiring clear consumer disclosures for cloning technologies.

The Los Angeles County Democratic Party is likewise supportive of SB 11:

The Los Angeles County Democratic Party (LACDP) considers and debates many bills submitted by legislators and organizations and have voted unanimously in support of SB 11. California and Los Angeles County have often been on the forefront of innovative policies that can at our best, serve as beacons for the nation. And yet, the implications and applications of Artificial Intelligence have left us playing catch up while synthetic content has the capacity to warp reality and perception and create real harm.
Our members appreciate the clarifications this bill will provide and the protections it will establish for use of synthetic content for false and criminal intent, and the consumer warning labels requirements on the Department of Consumer Affairs′ website.
Equally, our members very much welcome the Judicial Council review this bill requires to assess claims that A.I. manipulated evidence is finding its way into court proceedings. Obviously, it is a troubling claim which could further undermine public confidence in our judicial system.

Arguments in Opposition
A coalition of technology and business associations, led by the Chamber of Commerce, oppose this measure on two main grounds. First, they argue that the mandated warning is vague and problematic:

First, as drafted, we are unclear if the bill is intended to capture business to business activities, such as companies selling advertising services to other companies wherein the advertisement may include synthetic content. To that end, Proposed Section 22650 should be amended to expressly permit business partners / vendors to use our AI tools to generate content as well as authorize businesses to sell or develop such content for their business partners/vendors. The bill should also be amended to clarify what exactly it means by ″misuse″ for purposes of this warning.

We are also concerned about how broadly ″provides access to″ would be interpreted, and whether it would arguably require warnings even for internal usage of tools. To that end, we suggest striking that language or somehow significantly limiting this to only external uses of AI technologies designed to create synthetic content.

> Relatedly, we are also concerned that there is no understanding of what constitutes ″misuse″ for purposes of the warning to consumers that misuse of the technology may result in civil or criminal liability for the user. Given the obvious clear chilling effect of this type of warning, and this is not an area where the bill should be vague. That issue aside, we in fact fundamentally object to the notion that companies should be required a warning to users that their use of a Generative AI product could subject them to civil or criminal liability.

Second, they argue that SB 11 is premature given the recent passage of AB 1836 regarding digital replicas and the publicity rights of deceased individuals:

> 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 completely synthetic voice 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 synthetic voice 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[…].″
>
> It is unclear to us whether the intent here is to prevent companies from using synthetic voices to knowingly infringe likeness rights, but we note that the provision undercuts the ″knowingly″ requirement. To that end, there should be an exception if the likeness was truly unintentional.
>
> Take for example if a studio uses a synthetic voice 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 synthetic voice.
>
> Or take for example if a studio has evidence that it paid another actor for the right to use their voice, altered by AI, in a production. There may be no evidence that it intended to copy another actor′s voice, but if the synthetic voice unintentionally ends up sounding like this other actor that the studio potentially does not even know of, they could still be required to pay that other actor who has a similar voice.
>
> Yet, if an actor stars in a product and happens to have a voice similar to another individual or actor, the studio would not face these same issues.

FISCAL COMMENTS

According to the Assembly Appropriations Committee:

1) Possible costs (General Fund, special funds) to the Department of Justice (DOJ) of an unknown amount. Actual costs will depend on whether the Attorney General pursues enforcement actions, and, if so, the level of additional staffing DOJ needs to handle the related workload. If DOJ hires staff to handle enforcement actions authorized by this bill, it would incur significant costs, likely in the low hundreds of thousands of dollars annually at a minimum. If DOJ does not pursue enforcement as authorized by this bill, it would likely not incur any costs.

2) Cost pressures (Trial Court Trust Fund, General Fund) of an unknown but potentially significant amount to the courts to adjudicate civil actions and additional criminal charges, and to review the impact of AI technology on evidence and, if needed, issue related rules of court. Actual costs for adjudication will depend on the number of cases filed and the amount of court time needed to resolve each case. It generally costs approximately $1,000 to operate a courtroom for one hour. Judicial Council reports minor and absorbable costs to conduct the study and create rules of court.

   Although courts are not funded on the basis of workload, increased pressure on the Trial Court Trust Fund may create a demand for increased funding for courts from the General Fund. The fiscal year 2025-26 state budget provides $82 million ongoing General Fund to the Trial Court Trust Fund for court operations.

3) Costs (local funds, General Fund) to the counties and the California Department of Corrections and Rehabilitation to incarcerate people convicted of false impersonation offenses. Actual incarceration costs will depend on the number of convictions, the length of each sentence, and whether each sentence must be served in county jail or state prison. The average annual cost to incarcerate one person in county jail is approximately $29,000. The Legislative Analyst′s Office estimates the average annual cost to incarcerate one person in state prison is $133,000. County incarceration costs are not subject to reimbursement by the state. However, overcrowding in county jails creates cost pressure on the General Fund because the state has historically granted new funding to counties to offset overcrowding resulting from public safety realignment

VOTES

SENATE FLOOR: 38-0-2
YES: Allen, Alvarado-Gil, Archuleta, Arreguín, Ashby, Becker, Blakespear, Cabaldon, Caballero, Cervantes, Choi, Cortese, Dahle, Durazo, Gonzalez, Grayson, Grove, Jones, Laird, Limón, McGuire, McNerney, Menjivar, Niello, Ochoa Bogh, Padilla, Pérez, Richardson, Rubio, Seyarto, Smallwood-Cuevas, Stern, Strickland, Umberg, Valladares, Wahab, Weber Pierson, Wiener
ABS, ABST OR NV: Hurtado, Reyes

ASM JUDICIARY: 11-0-1
YES: Kalra, Dixon, Bauer-Kahan, Bryan, Connolly, Harabedian, Pacheco, Papan, Sanchez, Stefani, Zbur
ABS, ABST OR NV: Macedo

ASM PUBLIC SAFETY: 9-0-0
YES: Schultz, Alanis, Mark González, Haney, Harabedian, Lackey, Nguyen, Ramos, Sharp-Collins

ASM PRIVACY AND CONSUMER PROTECTION: 15-0-0
YES: Bauer-Kahan, Dixon, Bryan, DeMaio, Irwin, Lowenthal, Macedo, McKinnor, Ortega, Patterson, Pellerin, Petrie-Norris, Ward, Wicks, Wilson

ASM APPROPRIATIONS: 11-0-4

YES: Wicks, Arambula, Calderon, Caloza, Elhawary, Fong, Mark González, Ahrens, Pacheco, Pellerin, Solache
ABS, ABST OR NV: Sanchez, Dixon, Ta, Tangipa

UPDATED

VERSION: August 29, 2025

CONSULTANT: Shiran Zohar / JUD. / (916) 319-2334 FN: 0001369