Date of Hearing: June 30, 2026
Counsel: Kimberly Horiuchi

ASSEMBLY COMMITTEE ON PUBLIC SAFETY
Nick Schultz, Chair

SB 1111 (Ashby) – As Amended March 23, 2026

SUMMARY: Expands the crime of false impersonation to include any use of a digital replica with the intent to impersonate another. Specifically, **this bill**:

1) Includes "digital replicas" in the prohibitions against the unauthorized commercial use of name, voice, signature, photograph, or likeness (referred to as "right of publicity").

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

EXISTING LAW:

1) 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 not exceeding $1,000 or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment. (Pen. Code § 528.5, subd. (a) & (d).)

2) States that impersonation is credible if another person would reasonably believe, or did reasonably believe, that the defendant was or is the person who was impersonated. (Pen. Code § 528.5, subd. (b).)

3) Provides that every person who falsely personates another in either their private or official capacity, and in that assumed character carries out specified actions, is punishable by a fine not exceeding $10,000, imprisonment in a county jail not exceeding one year, or imprisonment in a county jail for 16 months, 2 or 3 years and/or a fine. (Pen. Code, § 529.)

4) Provides that every person who falsely personates 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.)

5) Prohibits any person from knowingly using 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 such person's prior consent, and may be liable for any damages sustained by the person or persons injured as a result thereof. (Civ. Code, § 3344, subd. (a).)

6) Defines "digital replica" to mean 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.)

7) Defines "artificial intelligence" to mean 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, subd. (a).)

FISCAL EFFECT: Unknown.

COMMENTS:

1) **Sponsor**: 11:11 Media

2) **Author's Statement**: According to the author, "California is leading the nation in AI regulations. However, a significant gap remains. The lack of a comprehensive legal framework to address the non-consensual creation of AI deepfake images leaves victims with no remedy. While some deepfakes target public figures, AI software now allows users to create content featuring anyone. Often, women are the targeted victims, and the vast majority of incidents are sexually explicit in nature.

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

3) **False Impersonation**: This bill expands the crimes of false impersonation to include conduct that relies on a digital replica. Penal Code section 528.5 punishes any person who knowingly and without consent credibly impersonates another actual person through or on an Internet Web site or by other electronic means for purposes of harming, intimidating, threatening, or defrauding another person. Penal Code section 529 punishes a person who falsely personates another in either his or her private or official capacity, and in that assumed character does any of the following: (a) becomes bail or surety for any party in any proceeding whatever, before any court or officer authorized to take that bail or surety; (b) verifies, publishes, acknowledges, or proves, in the name of another person, any written instrument, with intent that the same may be recorded, delivered, or used as true; or (c) does any other act whereby, if done by the person falsely personated, [they] might, in any event, become liable to any suit or prosecution, or to pay any sum of money, or to incur any charge, forfeiture, or penalty, or whereby any benefit might accrue to the party personating, or to any other person.

   An example of false personation would be a person who identified themselves to law enforcement as someone else for purposes of evading criminal liability. (See *People v.*

Chardon (1999) 77 Cal.App.4th 205.) Penal Code section 530 is false personation for purposes of stealing something of value. An example of this would be dressing up like a baggage handler to steal luggage or impersonating a long lost relative to obtain the victim's money. (*People v. Montalvo* (2019) 36 Cal.App.5th 597 [defendant dressed up like a police officer to effectuate a robbery].) This bill expands these offenses to include a person who engages in false personation via a digital replica.

4) **Background on Artificial Intelligence (AI) Issues**: Over the past five years, 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 is not surprising to see AI-generated images of public figures go viral or AI-generated reviews and comments on digital platforms. As such, generative AI models are raising concerns about the credibility of digital content and the ease of producing harmful content in the future. In an article published by the Brookings Institute, it is against the backdrop of technological advances, "civil society and policymakers have taken increasing interest in ways to distinguish AI-generated content from human-authored content."[1] The Brookings Institute goes on to explain that there are four suggested methods to determine if something is AI-generated[2]:

> There are several approaches that have been proposed for detecting AI-generated content. The four most prominent approaches are watermarking (in its various forms), which is the embedding of an identifiable pattern in a piece of content to track its origin; content provenance, which securely embeds and maintains information about the origin of the content in its metadata; retrieval-based detectors, where all AI-generated content is stored in a database that can be queried to check the origin of content; and post-hoc detectors, which rely on machine learning models to identify subtle but systematic patterns in AI-generated content that distinguish it from human-authored content.[3]

AI has created challenges for courts evaluating the admissibility, authenticity, and reliability of evidence. Realistic synthetic content, including deepfakes, AI-generated voice clones, and fabricated images, continues to appear in the courts, requiring courts to consider the reliability and fairness of generative AI material as evidence.

In May 2024, the Judicial Council established the AI Task Force to oversee the development of policy recommendations to the council on the use of AI in the judicial branch and coordinate the timely consideration and development of proposals and potential actions by

---

[1] Siddarth Srinivasan, *Detecting AI fingerprints: A guide to watermarking and beyond* (January 4, 2024) Brookings Institution, located at https://www.brookings.edu/articles/detecting-ai-fingerprints-a-guide-to-watermarking-and-beyond/
[2] *Ibid*.
[3] *Ibid*.

the judicial branch. On February 21, 2025, the Taskforce provided a presentation to the courts wherein it provided a summary of AI usage in courts: 19 courts are already using generative AI; 19 courts plan to start using generative AI; seven courts did not respond to a request for information. Additionally, six courts have an AI use policy in place; 21 courts are planning to create a policy; and several courts are waiting for a model policy from Judicial Council. Proposed model language includes rejection of any discriminatory generative AI and requires disclosure or watermark if generative AI outputs make up a substantial portion of a written or visual work provided to the public.[4]

The Legislature passed AB 1836 (Bauer-Kahan), Chapter 258, Statutes of 2024, which prohibited a person from producing, distributing, or making available the digital replica of a deceased personality's voice or likeness in an expressive audiovisual work or sound recording without prior consent from specified persons, essentially the personality's heirs or their assignees. Damages to an injured party may be for an amount equal to the greater of $10,000 or the actual damages suffered by a person controlling the rights to the deceased personality's likeness.

5) **AI Impact on 6th Amendment Right of Confrontation:** As noted above, Judicial Council convened a task force on AI in courts and as evidence. However, the use of AI in criminal law may affect the defendant's right to a fair trial because it may limit the defendant's ability to cross-examine a witness. In *People v. Lopez* (2012) 55 Cal.4th 569, the California Supreme Court addressed the impact of machine learning (a rudimentary form of generative AI) in the generation of an expert's report.

First, the right of confrontation prohibits the prosecution from relying on "testimonial" out-of-court statements unless the witness is unavailable to testify and the defendant had a prior opportunity for cross-examination. (*People v. Lopez, supra*, at p. 576, citing *Crawford v. Washington* (2004) 541 U.S. 36.) A statement is "testimonial" if: (a) it is made … by or to a law enforcement agent and (b) describes a past fact related to criminal activity for (c) possible use at a later trial. Conversely, a statement that does not meet all three criteria is not testimonial. (*Id*., at 577.)

Ultimately, the court in *Lopez* held that the portions of the expert's report that were generated by a form of machine learning was not testimonial.

> The critical portions of the non-testifying analyst's laboratory report were not made with the requisite degree of formality or solemnity to be considered testimonial. Although a laboratory assistant's notation on a chart linking defendant's name to a particular blood sample was admitted for its truth, it was not testimonial hearsay. The notation was nothing more than an informal record of data for internal purposes, as was indicated by a small printed statement near the top of the chart: "FOR LAB USE ONLY." Because the notation in the non-testifying analyst's laboratory report linking defendant's name to the blood

[4] https://courts.ca.gov/advisory-body/artificial-intelligence-task-force

> sample was not testimonial in nature, the defendant's right of confrontation was not violated. (*Lopez, supra,* at 585.)

Courts will continue to apply the same 6th Amendment right of confrontation analysis for AI. If the properly watermarked and unbiased generative AI is considered testimonial, it will likely not be admissible unless the person who developed the generative AI material is present and available to testify.

6) **Veto of SB 11**: This bill is similar to SB 11 (Ashby) from 2025, which was vetoed by the Governor. In this veto message, he wrote:

> I commend the author for working to ensure that our state is prepared for the challenges raised by AI's ability to produce highly realistic digital content. I share the author's concern over the risks posed by synthetic content, including the use of AI to impersonate or appropriate another's likeness without their consent. However, this bill also requires any AI technology that enables a user to create a digital replica to include, wherever a user may input a prompt, a hyperlink to a clear and conspicuous disclosure to warn users of potential civil or criminal liability. Failure to include the hyperlink exposes the technology provider to significant civil liability under this measure.
>
> This year, I have signed bills requiring companion chatbot operators to disclose to users that they are interacting with an artificial system (SB 243, Padilla) and internet companies to warn minors of the potential dangers of social media use (AB 56, Bauer-Kahan). Under certain circumstances, public disclosures and warning labels can play a key role in providing transparency to the public and mitigating harm. In this case, however, it is unclear whether a warning would be sufficient to dissuade wrongdoers from using AI to impersonate others without their consent.

However, this bill, while similar to SB 11, does not require a creator to include a hyperlink to a disclosure regarding civil and criminal liability. It simply includes digital replicas in statutes related to false impersonation and violations of the right of publicity statute.

7) **Argument in Support**: According to *11:11 Media*, "As artificial intelligence tools become more advanced and more accessible, it has become far too easy to create and spread nonconsensual AI-generated content. A person's voice or likeness can now be copied, manipulated, and used without their knowledge or consent. This abuse can be used to humiliate, harass, exploit, and impersonate people, causing serious emotional, reputational, and financial harm.

"This issue is urgent. AI-generated abuse is already being used to create sexually explicit deepfakes, spread false statements, and impersonate real people in deeply harmful ways. California's Department of Justice cites research showing that 90% of victims are women, 93% suffered significant emotional distress, 51% had suicidal thoughts, and 49% reported

being stalked or harassed online by people who saw the material. These harms disproportionately affect women and girls and increasingly affect children as well.

…

"SB 1111 is an important step to ensure California law keeps pace with this growing threat. It reflects a simple principle: people deserve protection when their voice or likeness is used without consent, including through AI-generated digital replicas. As technology moves faster than the law, California must act to protect victims and provide clearer paths to accountability. California has often led the nation in responding to new harms, and this bill continues that leadership. It sends a clear message that innovation cannot come at the expense of safety, dignity, and basic protections."

8) **Argument in Opposition**: None submitted.

9) **Related Legislation**: SB 11 (Ashby) would have ensured that computer-manipulated or generated content is incorporated into the right of publicity law and criminal false impersonation statutes. This bill requires those making available technology to provide a warning to consumers about liability for misuse, as provided. This bill also requires Judicial Council to review the impact of AI on evidence introduced in court proceedings and to adopt rules of court as necessary. SB 11 was vetoed by the Governor.

10) **Prior Legislation**:

a) AB 316 (Krell), Chapter 672, Statutes of 2025, established that in civil actions, where a plaintiff alleges harm caused by AI, a defendant who developed, modified, or used the AI is prohibited from asserting that the AI acted autonomously as a defense.

b) AB 1836 (Bauer-Kahan), Chapter 258, Statutes of 2024, 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.

c) AB 2602 (Kalra), Chapter 259, Statutes of 2024, limited the unauthorized use of digital replicas by providing that a provision in an agreement between an individual and any other person for the performance of personal or professional services is unenforceable only as it relates to a new performance, fixed on or after January 1, 2025, by a digital replica of the individual if the provision meets all of the specified conditions.

d) SB 942 (Becker), Chapter 291, Statutes of 2024, placed obligations on 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.

e) SB 970 (Ashby), of the 2023-24 Legislative Session, was similar to this bill and was held in the Senate Committee on Appropriations.

REGISTERED SUPPORT / OPPOSITION:

Support

11:11 Media Impact (Sponsor)
California Federation of Labor Unions, Afl-cio
California Initiative for Technology & Democracy, a Project of California Common CAUSE
Chamber of Progress
Common Sense Media
Rape, Abuse, & Incest National Network
Sag-aftra
Transparency Coalition.ai
1 Private Individual

Opposition

None submitted.

Analysis Prepared by: Kimberly Horiuchi / PUB. S. / (916) 319-3744