



## **SUMMARY**

SB 11 addresses artificial intelligence (AI) abuse by providing legal recourse for victims and requiring consumer warnings on AI cloning software. SB 11 also requires the Judicial Counsel to develop methods that identify AI generated evidence to protect the integrity of court proceedings. This bill strikes a balance between regulating rapidly advancing AI technologies and allowing continued innovation in the sector, while creating a remedy for AI abuse victims and protecting court proceedings across California.

## **BACKGROUND**

Artificial intelligence has pushed the boundaries of how machines function to make human lives easier. However, the lack of necessary regulations have led to its misuse.

In 2020 over 100,000 AI generated nude images of women were created, and an alarming number of deepfake videos consisted of AI generated pornography.<sup>1</sup> Over the past few years there have been numerous instances of deepfake videos and images that use high-profile individuals' name, image, and likeness (NIL) to spread misinformation and generate profit.

In response to these issues, Governor Newsom signed several AI bills into law during the 2023-24 legislative session. Some of these laws aim to prevent the expansion of AI child pornography and direct social media platforms to flag deepfake explicit content. Other bills focus on labeling online AI election deepfakes that use candidates' NIL to mislead voters.

Despite these efforts, existing law still does not provide victims with adequate pathways to seek remedies for their concerns.

## **THE PROBLEM**

The lack of a comprehensive legal framework for addressing the challenges posed by AI is dangerous. It leaves individuals vulnerable to various forms of exploitation including identity theft, scams, misinformation, and drastic misrepresentation of character.

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.

In one case, pornographic AI generated images of Taylor Swift gained over 45 million views on social media in a 17 hour period.<sup>2</sup> Similarly, AI was used to create fake explicit content of Billie Eilish.<sup>3</sup> Another incident falsely depicted Barack Obama making various claims that he did not say.<sup>4</sup>

While some deepfakes target public figures, easily accessible AI software now allow users to create non-consensual content featuring anyone. This issue predominantly impacts women and girls and has been difficult for victims to address, much less seek justice.

Over 9,500 websites have been identified that upload AI generated pornography. Of the deepfake videos found on these sites, over 95% are sexually explicit and feature women who did not consent to their creation.<sup>5</sup>

Additionally, about 90% of Americans say that altered videos and images cause harm by creating

<sup>2</sup> [National Sexual Violence Resource Center](#)

<sup>3</sup> [The Organization for Economic Cooperation and Development \(OECD\) Global Partnership on AI](#)

<sup>4</sup> [Department of Homeland Security](#)

<sup>5</sup> [National Sexual Violence Resource Center](#)

<sup>1</sup> [Department of Homeland Security](#)

doubt and uncertainty around the facts of current events and potentially controversial issues.<sup>6</sup> The rise in deepfake technology has led to a surge in fraudulent activities, with deepfake-related fraud cases more than doubling in the United States from 2022 to early 2023.<sup>7</sup>

Understanding and defining this technology is crucial to effectively regulating its misuse and protecting individuals from abuse and misinformation, while still supporting ethical innovation and advancement.

---

### THE SOLUTION

SB 11 addresses the continued exploitation of AI technologies. It is imperative to establish guardrails that protect consumers from harm and allow existing victims to seek recourse. This bill focuses on balancing innovation and individual privacy to prevent abuse through the following:

#### Establishing Penal Code Violations

- Clarifies that a person commits an offense if they knowingly use AI voice or video cloning technology to replicate another individual's name, voice, photograph, or likeness without such person's prior consent.

#### Legal Recourse for Victims

- Grants individuals the right to initiate civil litigation against parties who use AI cloning technology to replicate their name, voice, photograph, or likeness, leading to false personation.

#### Prevention of AI-Generated Evidence Tampering

- Directs Judicial Council to identify the impact of AI on evidence introduced in court proceedings and develop rules to help courts evaluate evidence generated or manipulated by AI, thus preserving the integrity of evidence presented to finders of fact in judicial evidentiary proceedings.

### Mandatory Consumer Warnings on AI Cloning Software

- Creates mandatory consumer warnings on AI cloning software, including warning requirements for all websites offering AI voice, image, or video cloning technology, and compliance monitoring overseen by the Department of Justice.

---

### SUPPORT

California Civil Liberties Advocacy  
California District Attorneys Association  
Chamber of Progress  
Common Sense Media  
Los Angeles County Democratic Party  
National AI Youth Council  
Recording Industry Association of America  
SAG-AFTRA  
The Center for AI and Digital Policy  
Transparency Coalition.AI

---

### FOR MORE INFORMATION

Lesley Brizuela, Legislative Director  
Email: [Lesley.Brizuela@sen.ca.gov](mailto:Lesley.Brizuela@sen.ca.gov)

Ryan Tomlinson, Legislative Aide  
Email: [Ryan.Tomlinson@sen.ca.gov](mailto:Ryan.Tomlinson@sen.ca.gov)

Phone: (916) 651-4008

---

<sup>6</sup> [Pew Research Center](#)

<sup>7</sup> [Forced Verification and AI/Deepfake Cases Multiply at Alarming Rates](#)