



September 25, 2024

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the last page or call your regular Skadden contact.

This memorandum is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum is considered advertising under applicable state laws.

One Manhattan West
New York, NY 10001
212.735.3000

300 S. Grand Ave., Suite 3400
Los Angeles, CA 90071
213.687.5000

California Enacts Host of AI-Related Bills Designed To Protect Individuals

In the absence of federal legislation addressing the development and deployment of artificial intelligence (AI) systems, individual states continue to fill that void by enacting state-specific legislation.

On September 17 and 19, 2024, California passed a series of laws related to AI, which:

- Protect against certain unauthorized use of digital replicas of an individual.
- Require that large AI developers watermark AI-generated images and provide tools to detect such images.
- Offer protection against certain sexually explicit digital content.

We discuss the key provisions of each of these new laws below.

Use of AI To Create an Individual's Digital Likeness

Two new California laws, [AB 2602](#) and [AB 1836](#), are designed to protect individuals from the unauthorized use of their voice and likeness through digital replicas (*i.e.*, computer-generated, highly realistic and readily identifiable representations of an individual's likeness). Although the laws do not mention AI explicitly, they were each clearly drafted to address AI-generated replicas.

Together, the two new laws offer certain protections against unauthorized digital replicas both during a person's lifetime and posthumously.

Contractual Protections for Using Digital Replicas

AB 2602 is designed to ensure that an individual has transparency into the use of their persona to create digital replicas and is adequately represented during contract negotiations. Under this new law, any contractual provision that permits the creation or use of a digital replica in lieu of work the individual would have otherwise performed must include a reasonably specific description of how the digital replica will be used (unless the usage is otherwise consistent with the terms of the professional services being offered by such individual).

If the contract does not include such a description, the provision may still be enforceable if the individual whose digital replica rights are being licensed is represented either by:

- legal counsel, with commercial terms that are clear and conspicuous and signed or initialed by the individual, or
- a labor union representing workers who do the proposed work, with their collective bargaining agreement expressly addressing uses of digital replicas (such as the SAG-AFTRA Agreement).

California Enacts Host of AI-Related Bills Designed To Protect Individuals

One notable aspect of AB 2602 is that it applies only to new performances fixed on or after January 1, 2025, meaning that the law will not retroactively affect digital replicas created or used before that date. This concession was made to accommodate studios and other content creators who initially opposed the bill due in part to concerns about the potential retroactive impact of the law.

Posthumous Use of Digital Replicas

AB 1836 amends existing protections for the posthumous use of an individual's persona to cover digital replicas.

“Digital replica” is defined as “a computer-generated, highly realistic electronic representation that is readily identifiable as the voice or visual likeness of an individual that is embodied in a sound recording, image, audiovisual work, or transmission in which the actual individual either did not actually perform or appear, or the actual individual did perform or appear, but the fundamental character of the performance or appearance has been materially altered.”

The law grants legal rights to estates, allowing them to control and protect the use of a deceased person's digital replica for up to 70 years after their death. More specifically, anyone who produces, distributes or makes available a digital replica of a deceased person's likeness or voice in an audiovisual work or sound recording without prior consent from the applicable rightsholder (e.g., the deceased individual's surviving spouse, children or grandchildren) is liable for the greater of the actual damages suffered by the injured rightsholder or a minimum of \$10,000.

The rights conferred under AB 1836 are considered property rights, meaning they can be transferred or inherited by contract, trust or other testamentary instruments.

Notably, AB 1836 includes several exemptions where consent would not be required. These track “fair use” type principles and include use of a person's digital replica:

- In connection with any news, public affairs or sports broadcast or account.
- For purposes of comment, criticism, scholarship, satire or parody.
- As a representation of the individual in a documentary or in a historical or biographical manner, 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.
- In a manner that is fleeting or incidental.
- In an advertisement or commercial announcement for a work that falls into any of the foregoing exemptions.

Earlier in 2024, Tennessee enacted the [ELVIS Act](#) and Illinois amended its Right of Publicity Act to offer similar protections.

AI Detection and Watermarking

The California AI Transparency Act ([SB 942](#)) is designed to make the identification of AI-generated content more transparent to users by requiring developers of widely used AI systems to provide certain AI-detection tools and watermarking capabilities.

The Act's obligations apply to “covered providers,” defined as any “person that creates, codes, or otherwise produces a generative artificial intelligence system that has over 1,000,000 monthly visitors or users” and is publicly accessible within California.

AI-Detection Tools

Covered providers must offer users a free, AI-detection tool that allows users to upload content and determine whether an image, video or audio content was created or altered by the provider's generative AI system. The tool must also output any provenance data (i.e., embedded data that verifies the digital content's authenticity, origin or history of modifications) that is detected in such content.

The tool must, however, block any personal information (as defined in the California Consumer Privacy Act) that is included in the provenance data, and also, generally speaking, cannot collect or retain any personal information from users of the tool. Note that there is no affirmative obligation for the covered provider to create any provenance data or ensure it is present in AI-generated content, and the tool is not required for text content.

Covered providers must also collect user feedback related to the efficacy of the tool and use such feedback to improve it.

Watermarking

Covered providers must offer users the option to include conspicuous disclosures in image, video or audio content that is created or altered using such provider's generative AI system that identifies such content as AI-generated. Further, the disclosure must be “clear, conspicuous, [and] appropriate” for the content medium and must be permanent or “extraordinarily difficult to remove” to the extent technically feasible.

In addition, even if a user does not exercise the option to include the conspicuous disclosure, covered providers must include a “latent” (i.e., present but not manifest) disclosure in image, video or audio content that is created by such provider's generative AI system.

California Enacts Host of AI-Related Bills Designed To Protect Individuals

Such latent disclosure must be permanent or extraordinarily difficult to remove and must include, to the extent technically feasible and reasonable:

- The name of the covered provider.
- The name and version number of the generative AI system that created or altered the content.
- The time and date of the content's creation or alteration.
- A unique identifier.

As with the AI-detection tool requirement, the watermarking requirement does not apply to text content.

Notably, if a covered provider licenses its generative AI system, such covered provider must contractually obligate the licensee to maintain such generative AI system's ability to include the latent disclosure detailed above in content that the system creates or alters.

In the event the covered provider knows that the licensee is not in compliance with such obligation, the covered provider must revoke the license within 96 hours of discovering such breach, and the licensee must subsequently cease use of the licensed generative AI system.

Penalties

Covered providers who are in violation of the California AI Transparency Act are liable for a civil penalty of \$5,000 per violation, and each day that a covered provider is in violation is considered a discrete violation.

If a licensee fails to cease use of a generative AI system after the license has been revoked, a county counsel or city attorney may bring a civil action for both injunctive relief and reasonable attorney's fees and costs.

Exclusions

The California AI Transparency Act does not apply to any product, service, internet website or application that provides exclusively nonuser-generated video game, television, streaming, movie or interactive experiences.

Although the California AI Transparency Act does not become operative until January 1, 2026, it marks a significant step forward in creating a more transparent and responsible future with respect to generative AI and highlights the role both individual users and generative AI companies play in helping shape this future.

Policing Sexually Explicit Digital Content

California also enacted two bills, [SB 926](#) and [SB 981](#), aimed at the creation and distribution of sexually explicit digital content. The increasing deployment of AI systems has increased concerns that malicious actors will use such technology to generate falsified sexually explicit images and videos without consent. Although neither bill explicitly mentions AI, they nonetheless cover this technology.

Creation and Distribution of Sexually Explicit Content (SB 926)

SB 926 makes it illegal to intentionally create and distribute any photorealistic, digital or computer-generated image or other pictorial representation of an intimate body part of another identifiable person, or of a person engaged in a sexual act that a reasonable person would believe is authentic.

Notably, the "identifiable" requirement only means capable of identification or capable of being recognized, including by the victims themselves. The victim's identity does not need to be established.

Additionally, under the bill, in order for such conduct to be illegal, the individual who distributes such image must know or should know that distribution of the image will cause serious emotional distress, and the person depicted must suffer such distress.

Reporting Sexually Explicit Digital Identity Theft (SB 981)

SB 981 obligates social media platforms to establish a reporting mechanism through which users of such platforms can report sexually explicit digital identity theft. "Social media platform" is generally defined as a public or semipublic internet-based service or application that has users in California and that meets both of the following criteria:

- A substantial function of the service or application is to connect users in order to allow them to interact socially with each other within the service or application.
- The service or application allows users to:
 - Construct a public or semipublic profile for purposes of signing into and using the service or application.
 - Populate a list of other users with whom an individual shares a social connection within the system.
 - Create or post content viewable by other users, including, but not limited to, on message boards, in chat rooms or through a landing page or main feed that presents the user with content generated by other users.

California Enacts Host of AI-Related Bills Designed To Protect Individuals

However, such definition does not include stand-alone direct messaging services that provide end-to-end encrypted communication or the portion of a multiservice platform that uses end-to-end encrypted communication.

Sexually explicit digital identity theft means the posting of “covered material” on a social media platform. In order to qualify as covered material:

- the material must be an image or video created or altered through digitization that would appear to a reasonable person to be an image or video of an intimate body part of an identifiable person or an identifiable person engaged in certain sexual acts,
- the person reporting such material must be the person depicted in the material, and such person did not consent to the use of their likeness in the material, and
- the material must be displayed, stored or hosted on the social media platform.

While the social media platform is investigating a reported instance of sexually explicit digital identity theft, the platform must temporarily block such identity theft from being publicly

viewable on the platform. If it is determined that the reported identity theft meets the definition of sexually explicit digital identity theft, it must immediately be removed.

Generally speaking, the social media platform must determine within 30 days of confirming receipt of a user’s report whether there is a reasonable basis to believe that the reported sexually explicit digital identity theft meets the definition under the bill.

If the social media platform is unable to comply with the foregoing obligation due to circumstances beyond its reasonable control, it has 60 days from the date the covered material was first reported to make such determination, and it must provide the reporting user with notice of such delay.

In Sum

The enactment of these laws, coupled with other California laws that were recently put in place to address the use of AI in connection with elections, is another example of how states are taking proactive steps to regulate certain uses of AI.

In the absence of federal legislation, we expect to see an increasing number of state-specific AI-related legislation.

Contacts

M. Oren Epstein

Partner / New York
212.735.2517
oren.epstein@skadden.com

Stuart D. Levi

Partner / New York
212.735.2750
stuart.levi@skadden.com

Glen G. Mastroberte

Partner / Los Angeles
213.687.5699
glen.mastroberte@skadden.com

Priya R. Matadar

Associate / New York
212.735.2542
priya.matadar@skadden.com

Shannon N. Morgan

Associate / New York
212.735.3711
shannon.morgan@skadden.com