California's legislative session came to a close with the adoption of a torrent of bills concerning artificial intelligence (AI) as well as updates to the state's broad consumer privacy law, the California Consumer Privacy Act (CCPA). Conversely, other AI and privacy legislation did not make it out of the legislature or was vetoed. In all, Governor Newsom signed over a dozen AI and privacy bills, while vetoing a handful. Below we summarize some of the most notable AI and privacy bills enacted and vetoed.

AI Bills Enacted

SB 942 - California AI Transparency Act

SB 942 requires producers of generative AI (genAI) systems that are publicly available in California with over one million monthly visitors or users (covered providers) to provide a free "AI detection tool" that users may employ to assess whether content was created or altered by the provider's genAI system. The detection tool also must provide any system provenance data detected in the content (i.e., embedded data that verifies the digital content's authenticity, origin, or history of modifications) but it must not provide any personal provenance data detected in the content (i.e., personal or device-specific information). The detection tool must allow users to upload content or provide a URL to link to online content.

Covered providers must also offer users the option to include "manifest" disclosures in content created or altered by the genAI system. A "manifest" disclosure is a clear and conspicuous disclosure that identifies the content as AI-generated, is appropriate to the medium, and is understandable to a reasonable person. To the extent technically feasible, the disclosure must be permanent or "extraordinarily difficult" to remove. Covered providers must also include in content created or altered by the genAI system a "latent" disclosure (i.e., an embedded watermark that is not manifest to natural persons). To the extent technically feasible and reasonable, the latent disclosure must convey the name of the covered provider, the name and version number of the genAI system, the date and time of the creation or alteration of the content, and a unique identifier. The disclosure must be permanent or "extraordinarily difficult" to remove, must be identifiable by the covered provider's AI detection tool, and must be consistent with widely accepted industry standards. If the covered provider licenses its system to a third party, it must contractually mandate the third party to maintain the AI system's capability to include the latent disclosure. If the covered provider knows that the licensee has disabled the capability, it must revoke the license within 96 hours.

SB 942 comes into effect January 1, 2026.

AB 2013 - AI Training Data Transparency

To increase transparency about the data used to build AI systems, AB 2013 requires developers of genAI systems or services that are publicly available in California to post a "high-level summary" of the datasets used in the development of the system or service, including the following information:

- The sources or owners of the datasets;
- A description of how the datasets further the intended purpose of the artificial intelligence system or service;
- The number of data points included in the datasets, which may be in general ranges, and with estimated figures for dynamic datasets;
- A description of the types of data points within the datasets, including whether:
    - the datasets include any data protected by copyright, trademark, or patent, or whether the datasets are entirely in the public domain;
    - the datasets were purchased or licensed by the developer;
    - the datasets include personal information under the CCPA;
    - the datasets include aggregate consumer information under the CCPA; or
    - there was any cleaning, processing, or other modification to the datasets by the developer, including the intended purpose of those efforts in relation to the artificial intelligence system or service.
- The time frame during which the data in the datasets were collected;
- The dates the datasets were first used during the development of the AI system or service; and
- Whether the genAI system or service used or continuously uses synthetic data generation in its development.

These requirements apply regardless of whether the system or service is provided for a fee. There are exceptions for genAI models focused on security and integrity; those focused on the operation of an aircraft in national

airspace; and those developed for national security, military, or defense purposes and only available to a federal entity. For a more extensive analysis, see here.

For systems released on or after January 1, 2022, such disclosures must be made on or before January 1, 2026. After that time, developers must make the disclosures before a genAI system or a substantial modification to a genAI system is made publicly available.

AB 3030 - AI in Health Care Services

AB 3030 requires any health facility, clinic, physician's office, or office of a group practice that uses genAI to generate written or verbal patient communications pertaining to the patient's clinical information to ensure that those communications include a disclaimer that indicates that the communication was generated by genAI, as follows:

- For written communications involving physical and digital media, such as letters and emails, the disclaimer must appear prominently at the beginning of each communication;
- For written communications involving continuous online interactions, such as chat-based telehealth, the disclaimer must be prominently displayed throughout the interaction;
- For audio communications, the disclaimer must be provided verbally at the start and the end of the interaction; and
- For video communications, the disclaimer must be prominently displayed throughout the interaction.

In addition, the communications must include clear instructions that describe how a patient may contact a human health provider, employee of the health facility, clinic, physician's office, office of a group provider, or another appropriate person.

The law exempts communications that are generated by genAI and read and reviewed by a human licensed or certified health care provider.

CA 3030 comes into effect January 1, 2025.

AB 2355, AB 2655, AB 2839 - Use of Deepfakes in Elections

California adopted a series of bills to protect against the misleading use of "deepfakes" in elections (for a more extensive discussion, see here).

AB 2355 requires "qualified political advertisements"—defined as advertisements "that contain any image, audio, or video that is generated or substantially altered using artificial intelligence"—to include disclosures specifying that the advertisement was generated or substantially altered using AI. AB 2355 provides that something is "generated or substantially altered using artificial intelligence" if it is "entirely created using artificial intelligence and would falsely appear to a reasonable person to be authentic or materially altered by artificial intelligence such that a reasonable person would have a fundamentally different understanding of the altered media when comparing it to an unaltered version." AB 2355 comes into effect January 1, 2025.

AB 2655, the Defending Democracy from Deepfake Deception Act of 2024, requires large online platforms with at least one million California users to remove, or to label as manipulated, "materially deceptive content" related to elections in California during the 120 days prior to an election and throughout the day of the election. Additionally, the bill requires these platforms to label certain content inauthentic, fake, or false during these periods prior to and through elections in California. "Materially deceptive content" is defined as "audio or visual media that is digitally created or modified, and that includes, but is not limited to, deepfakes and the output of chatbots, such that it would falsely appear to a reasonable person to be an authentic record of the content

depicted in the media." AB 2655 comes into effect January 1, 2025.

[AB 2839](#) expands existing law regarding the distribution of deceptive content about a candidate to prohibit any person, committee, or entity from knowingly, and with malice, distributing an advertisement or other election communication containing certain types of "materially deceptive content" within certain periods of time around an election. A federal district court has preliminarily enjoined the law on First Amendment grounds. AB 2839 came into effect immediately following adoption.

[AB 2602](#), [AB 1836](#) - Protecting Computer-Generated Likenesses

Two bills signed into law protect the use of computer-generated likenesses, so-called "digital replicas" (for more in-depth discussion of both bills, see [here](#)).

[AB 2602](#) makes a contractual provision unenforceable when 1) the provision involves the creation and use of a digital replica of the individual's voice or likeness in place of work the individual would otherwise have performed in person; 2) the provision does not include a reasonably specific description of the intended uses of the digital replica; and 3) the individual was not represented by legal counsel negotiating the individual's digital replica rights or a labor union whose collective bargaining agreement expressly addresses use of digital replicas. AB 2602 comes into effect January 1, 2025.

[AB 1836](#) prohibits the use of a digital replica of a deceased personality's voice or likeness in an expressive audiovisual work or sound recording without prior consent, with exceptions for uses in connection with (1) news, public affairs, or sports broadcasts; (2) comment, criticism, scholarship, satire, or parody; (3) representation of the individual as themselves in a documentary or in a historical or biographical manner, including some degree of fictionalization; (4) a fleeting or incidental use; or (5) advertisements or commercial announcements for any of the above. AB 1836 comes into effect January 1, 2025.

Privacy Bills Enacted

[AB 1008](#) - Amending CCPA Definition of "Personal Information" to Include "Abstract Digital Formats"

Framed as a "clarification" of existing law, [AB 1008](#) modifies the definition of "personal information" in the CCPA by expressly providing that personal information "can exist" in "abstract digital formats" including "artificial intelligence systems that are capable of outputting personal information." The [Assembly Floor Analysis](#) explained the bill was designed to clarify that if a genAI model is capable of "outputting personal information," then the company that provides the genAI system may constitute a data broker under the CCPA and, if the company sells access to its model, that sale may qualify as a "sale" of personal information under the CCPA. AB 1008 comes into effect January 1, 2025.

[SB 1223](#) - "Neural data" Deemed Sensitive Personal Information

[SB](#) 1223 amends the CCPA by expressly defining "sensitive personal information" to include a consumer's neural data, defined as "information that is generated by measuring the activity of a consumer's central or peripheral nervous system, and that is not inferred from nonneural information," subject to the right to limit the use and disclosure of sensitive personal information. Earlier this year, Colorado also expanded its definition of "sensitive data" to include "biological data" in its comprehensive consumer privacy law (see [H.B. 24-1058](#)). SB 1223 comes into effect January 1, 2025.

[AB 1824](#) - Recognizing Prior Opt-Outs in M&A Deals

[AB 1824](#) amends the CCPA to generally require that when a business acquires personal information as part of a merger, acquisition, bankruptcy, or other transaction, it as the transferee must honor opt-out requests previously made to the transferor. AB 1824 comes into effect January 1, 2025.

[AB 3286](#) - Adjustment of CCPA Monetary Thresholds

[AB 3286](#) (signed into law in mid-July) amends the CCPA to require the California Privacy Protection Agency to adjust monetary thresholds of specified provisions in the law every odd-numbered year, starting January 1, 2025, to reflect increases in the Consumer Price Index (CPI). Previously, this responsibility had fallen on the California Attorney General.

Vetoed AI and Privacy Bills

Notably, Governor Newsom returned three bills without his signature: SB 1047, AB 3048, and AB 1949.

[SB 1047](#) would have mandated that developers of large AI models, using computing power exceeding (10^{26}) integers, implement safety and security protocols. In vetoing the measure, Governor Newsom [explained](#) that regulating only the largest models could create a false sense of security regarding model safety, and expressed concern that the bill looked at the size of the system but ignored whether it was deployed in high-risk environments or involved critical decision-making or the use of sensitive data. For a more extensive discussion, see [here](#).

[AB 3048](#) would have required operating system developers to include an opt-out signal for personal information sharing. In vetoing the bill, Governor Newsom [cited](#) concerns over imposing design mandates on developers.

[AB 1949](#) would have amended the CCPA to require businesses to distinguish between adult and minor consumers at data collection. In vetoing the measure, Governor Newsom [expressed concern](#) that this significant change to the CCPA would have "unanticipated and potentially adverse effects on how businesses and consumers interact with each other, with unclear effects on children's privacy."

* * * * *

The raft of legislation reflects extraordinary attention and focus on AI and privacy issues. In adopting over a dozen new laws, California has clearly signaled its intent to play a significant role in establishing the rules of the road governing the deployment of genAI, creating significant new legal obligations on AI developers. It also has further strengthened the CCPA with respect to AI and on several discrete topics.

Authors

[Janis Kestenbaum](#)

Partner
JKestenbaum@perkinscoie.com

Peter Hegel

Counsel
PHegel@perkinscoie.com   312.324.8683

Rohan Andresen

Associate
RAndresen@perkinscoie.com

Francys Guevara

Associate
FGuevara@perkinscoie.com

Explore more in

Privacy & Security   Artificial Intelligence & Machine Learning
Blog series

Perkins on Privacy

Perkins on Privacy keeps you informed about the latest developments in privacy and data security law. Our insights are provided by Perkins Coie's Privacy & Security practice, recognized by Chambers as a leading firm in the field.

View the blog