

CLIENT ALERT | October 15, 2025

# California Assumes Role as Lead US Regulator of AI

***California enacts more than a dozen AI laws, including ones that impose new obligations on frontier developers in the name of greater transparency.***

## **Key Points:**

- Senate Bill 53 (SB 53), known as the Transparency in Frontier Artificial Intelligence Act, is a first-of-its-kind AI safety and transparency law that reflects California's continued efforts to stay at the forefront of AI regulation in the US.
- SB 53 primarily requires large frontier developers to draft and implement protocols to manage and mitigate catastrophic risk, publish transparency reports disclosing information about their frontier models, and establish regular reporting to California regulators regarding critical safety incidents, among other things.
- Governor Gavin Newsom signed or vetoed more than a dozen other bills passed by the California legislature that address AI issues such as companion chatbots, automated decision-making, data privacy, algorithmic pricing, and deepfakes and digital replicas. The governor also signed a bill delaying the implementation of the California AI Transparency Act, which was originally scheduled to go into effect in January 2026.

On October 13, 2025, California Governor Gavin Newsom [signed into law](#) a number of new bills that will either directly or indirectly implicate how companies use and deploy artificial intelligence (AI), while vetoing a handful of others. For developers of frontier models, the most notable law is SB 53, known as the Transparency in Frontier Artificial Intelligence Act, which Governor Newsom signed on September 29, 2025.

By passing SB 53, California becomes the first state in the US to directly regulate developers of "frontier" foundation models — that is, companies that develop AI models trained with more than  $10^{26}$  floating-point operations. This marks a different approach from statutes such as the Colorado AI Act, which have taken a risk-based approach to regulating the development and downstream deployment of "high-risk artificial intelligence systems." Instead, SB 53 focuses primarily on the *development* of frontier models.

This Client Alert analyzes the obligations and potential impact of SB 53 on generative AI developers. It also highlights the other AI-focused bills that passed the California legislature and were either signed or vetoed by the governor.

## Senate Bill 53 – Transparency in Frontier Artificial Intelligence Act

### Overview

At its core, SB 53 requires frontier developers to:

- Publish and keep current an enterprise-wide “frontier AI framework” that explains how the company identifies, assesses, and mitigates catastrophic risks, incorporates national and international standards, secures unreleased model weights, and governs internal use of frontier models, among other things
- Release detailed public transparency reports summarizing model capabilities, intended uses, risk-assessment results, third-party evaluations, and mitigation measures
- Submit rolling summaries of internal catastrophic-risk assessments and report any “critical safety incidents” to the California Office of Emergency Services (OES) within specified time periods
- Maintain robust whistleblower channels and non-retaliation policies, backed by a private right of action and fee-shifting for whistleblowers whose rights are violated
- Face civil penalties of up to \$1 million for violations, enforced by the California Attorney General

SB 53, which was sponsored by California Senator Scott Wiener, is a streamlined successor to Senator Wiener’s controversial Senate Bill 1047, which passed the legislature in 2024 but was ultimately vetoed by Governor Newsom. That bill similarly focused on preventing foundation AI models and their derivatives from causing “critical harms,” but deviated by imposing larger penalties and obligating developers to take steps to prevent downstream misuse of their models. Conversely, SB 53 asks developers to help identify and mitigate risks of critical harms through policymaking and reporting, but does not impose downstream liability on those developers.

### Scope and Application

SB 53 will establish a first-of-its-kind regulatory framework for developers of frontier models. Under the bill, a “frontier developer” is anyone who has trained or initiated the training of a “frontier model,” defined as a foundation model that was trained using a quantity of computing power greater than  $10^{26}$  integer or floating-point operations. While a number of SB 53’s provisions apply to all frontier developers, the bulk of its obligations apply solely to “large” frontier developers, which are frontier developers that, together with affiliates, collectively had annual gross revenues in excess of \$500 million in the preceding calendar year.

Notably, SB 53 requires the California Department of Technology to annually assess whether the definitions of “frontier model,” “frontier developer,” and “large frontier developer” should be updated so as to accurately reflect the latest developments in technology, scientific literature, and national and international standards. Accordingly, SB 53’s scope could evolve over time, and developers should continue to monitor its application to understand what obligations they may have.

## Obligations for All Frontier Developers

SB 53 contains a few requirements that apply to all frontier developers regardless of their annual revenues. Of note, SB 53 requires every frontier developer to publish a “transparency report” on its website either before or concurrently with the deployment of a frontier model that includes, among other things, the model’s release date, the forms of output that the model supports, intended uses/restrictions on use of the model, and a mechanism that would allow a user to communicate with the developer. Frontier developers are required to report critical safety incidents involving their models to the California OES within specified timeframes.

SB 53 also creates whistleblower protections for frontier developers’ “covered employees,” defined as employees responsible for assessing, managing, or addressing critical safety incidents. These employees must be allowed to make internal or external disclosures (including to the California Attorney General or federal regulators) about substantial dangers to public safety or violations of SB 53 without retaliation.

## Additional Obligations for Large Frontier Developers

While all frontier developers are required to abide by the requirements described above, SB 53 imposes an additional set of obligations on large frontier developers:

### Adoption of a Frontier AI Framework

SB 53 requires each large frontier developer to design, implement, and publicly publish a frontier AI safety and security framework describing how the developer assesses and mitigates catastrophic risks<sup>1</sup> associated with the use of its models. As noted in the statute, this framework should describe:

- **Adoption of Standards and Governance Practices:** How the developer integrates national, international, and industry best practices into its AI framework and establishes internal governance to ensure process implementation.
- **Risk Assessment:** How the developer identifies, evaluates, and mitigates potential catastrophic risks of frontier models (including risks from internal use of those models), as well as how the developer engages third parties to help assess catastrophic risks and mitigation effectiveness.
- **Pre- and Post-Deployment Review:** How the developer reviews assessments and adequacy of mitigations before deploying a frontier model, as well as how the developer decides whether and when to update the AI framework after deploying a frontier model.
- **Cybersecurity Measures and Incident Responses:** How the developer secures model weights against unauthorized access or modification and addresses any critical safety incidents.

SB 53 requires each large frontier developer to review its frontier AI framework at least annually and make updates as appropriate.

### **Catastrophic Risk Assessments, Regulatory Reporting, and Whistleblower Protections**

Under SB 53, large frontier developers must conduct assessments of catastrophic risk associated with their frontier models, the results of which must be published in the developer's public transparency report along with any other steps the developer has taken to fulfill the requirements of its frontier AI framework.

Large frontier developers must also establish a regular reporting cycle with the California OES to summarize assessments of catastrophic risk associated with internal use of its frontier model.

Finally, large frontier developers are required to create a process through which potential whistleblowers can anonymously submit information on potential catastrophic risk directly to the developer.<sup>2</sup>

### **Penalties**

Violations of a frontier developer's obligations relating to frontier AI frameworks and transparency or critical safety reporting are subject to civil penalties of up to \$1 million per violation.

Violations of SB 53's whistleblower provisions are subject to civil action by the whistleblower, who may be awarded damages, injunctive relief, and attorneys' fees and costs.

### **Strategic Implications for Developers**

SB 53 represents a paradigm shift in the regulatory treatment of advanced AI development in the US. Companies training large-scale foundation models will need to undertake significant compliance preparation, including mapping their model assets; creating, implementing, and documenting risk management frameworks; establishing effective and repeatable processes for risk assessment, incident monitoring, and regulatory reporting; and creating internal incident reporting procedures and training staff on new whistleblower protections. Penalties are steep — just a single violation is subject to a seven-figure fine — so it is critical that frontier developers that fall within SB 53's scope work closely with counsel to develop a fulsome compliance program.

Moreover, SB 53's requirements to publish safety frameworks and disclose risk assessments will force developers to balance their new transparency obligations with the risk of disclosing sensitive intellectual property and trade secrets. SB 53 does permit developers to redact certain sensitive information from publicly posted documents, but frontier developers should implement adequate review processes to ensure proprietary data is not inadvertently disclosed.

SB 53's whistleblower provisions could also heighten legal and reputational risk. Companies will need to implement internal reporting mechanisms and revise employment policies to incorporate anti-retaliation protections.

Finally, even developers of AI systems that are below SB 53's model scale or developer revenue thresholds should monitor their growth trajectories. Because SB 53's obligations trigger once a company crosses defined thresholds, developers approaching frontier scale should begin building compliance

infrastructure well in advance. They should also keep in mind that SB 53 has a built-in mechanism to revise the key definitions that define SB 53's scope in order to keep pace with changes in AI, so just because a developer is not in scope today does not mean they will not find themselves within the ambit of SB 53 in the future.

## **Governor Newsom Signs a Number of Other AI Bills, Vetoes Several Others**

In addition to SB 53, the California legislature passed more than a dozen other AI-focused bills in September 2025 that were sent to Governor Newsom for action. While the governor signed the bulk of the AI bills that reached his desk, he did veto a handful of bills, including SB 7, which would have regulated the use of automated decision-making tools in the employment context. Below is a brief overview of the most notable bills that Governor Newsom signed or vetoed:

### **Signed Into Law**

Governor Newsom signed the following AI bills into law:

- **Transparency**
  - **AB 853:** Delays the implementation of the California AI Transparency Act from January 1, 2026, to August 2, 2026. Among other things, the California AI Transparency Act (which passed last year as SB 942) requires providers of highly trafficked generative AI models to provide users with a free AI detection tool and to include certain provenance data in content generated by their models. Governor Newsom's signing message for AB 853 acknowledged that the California AI Transparency Act, "while well intentioned, present[s] implementation challenges" and encouraged "the Legislature to enact follow-up legislation in 2026, before the law takes effect, to address these technical feasibility issues." As a result, AI providers should expect further legislation on this topic next year.

AB 853 also adds new provisions to the California AI Transparency Act, including a requirement that large online platforms provide users with an interface to disclose the availability of system provenance data that indicates whether content was generated or substantially altered by a generative AI system. Additionally, capture device manufacturers — defined as any person or company that produces a device that can record photographs, audio, or video — are required to give users the option to embed certain latent disclosures in content, including the name and version number of the capture device and the time and date that the content was created.

- **Companion Chatbots**
  - **SB 243:** Requires operators of companion chatbots<sup>3</sup> to (i) provide clear and conspicuous notice to users indicating that the companion chatbot is not human; (ii) maintain a protocol for preventing the production of suicidal ideation, suicide, or self-harm content to a user; and (iii) for minor users, provide a notification every three hours that the system is not human and

encouraging the user to take a break, and prevent the production of sexually explicit material to the user. The bill also requires annual reports to the California Office of Suicide Prevention detailing the number of times the operator has referred users to crisis services as well as protocols regarding self-harm and suicidal ideation.

Notably, SB 243 does *not* apply to: (i) chatbots that are used “only for customer service, a business’ operational purposes, productivity and analysis related to source information, internal research, or technical assistance,” (ii) chatbots that are a feature of video games and that only reply to topics related to such video games, or (iii) a stand-alone consumer electronic device that functions as a speaker and voice command interface, acts as a voice-activated virtual assistant, and does not sustain a relationship across multiple interactions or generate outputs that are likely to elicit emotional responses in the user.

- **Algorithmic Pricing**

- **AB 325:** Prohibits a person from using or distributing a common pricing algorithm as part of a contract, combination in the form of a trust, or conspiracy to restrain trade or commerce. AB 325 also makes it unlawful for a person to use or distribute a common pricing algorithm if the person coerces another to set or adopt a recommended price or commercial term for the same or similar products or services.

- **Privacy / Cybersecurity**

- **SB 361:** Amends the California Consumer Privacy Act of 2018 (CCPA) and the California Privacy Rights Act of 2020 (CPRA) to enhance consumer privacy protections, particularly concerning data brokers.<sup>4</sup> Among other things, the bill requires data brokers to disclose certain information when registering with the California Privacy Protection Agency, including whether the data broker has shared or sold consumers’ data to a developer of a generative AI system or model in the past year.
- **AB 979:** Calls for the California Cybersecurity Integration Center to develop, by January 1, 2027, a California AI Cybersecurity Collaboration Playbook to facilitate information-sharing across cyber and AI communities and to strengthen collective cyber defenses against emerging threats, including AI. In producing the playbook, the California Cybersecurity Integration Center must consider federal requirements, standards, and industry best practices, including the Joint Cyber Defense Collaborative AI Cybersecurity Collaboration Playbook.
- **SB 446:** Requires companies that own or license computerized data containing personal information to disclose data breaches to any California resident whose personal data is reasonably believed to have been acquired by an unauthorized person.

- **Healthcare**

- **AB 489:** Prohibits AI developers and deployers from using specified terms, letters, or phrases in the advertising or functionality of an AI system that indicates or implies that the advice offered by the AI system is being provided by a licensed healthcare professional.

- **Digital Replicas / Deepfakes**

- **AB 621:** Creates a civil cause of action for a person depicted in sexually explicit deepfake materials without their consent against any person that intentionally discloses such materials or knowingly facilitates or aids in the distribution of such materials.

The law also creates potential liability for any person or company that provides a service that “enables the ongoing operation of a deepfake pornography service,” provided that the person both (i) receives evidence from a depicted individual or prosecutor that the person is providing services that enable the ongoing operation of a deepfake pornography service, and (ii) fails to take steps necessary to stop providing such services within 30 days.

- **SB 857:** Omnibus public safety bill that includes provisions relating to the generation of sexually explicit AI material. Specifically, the bill makes it a felony subject to prison and civil fines for knowingly sending or otherwise possessing in California any obscene material that contains a digitally altered or AI-generated depiction of a minor engaging in sexual conduct.

- **Real Estate**

- **AB 723:** Requires real estate brokers or salespersons to include a conspicuous statement in advertisements or promotional materials for the sale of real property indicating when an advertising image for such property has been digitally altered, including by AI, and providing a URL or QR code that directs an individual to the unaltered version of the image.

- **Legal System / Law Enforcement**

- **AB 316:** Prohibits defendants in civil actions who developed, modified, or used an AI system that caused harm to a plaintiff from arguing as a defense that the AI system autonomously caused such harm.
- **SB 524:** Requires law enforcement agencies to include disclosures in any official reports generated in whole or in part by AI. SB 524 also requires the agency to retain the first draft of the report and maintain an audit trail for as long as the official report is retained.

## Vetoed

Among the bills Governor Newsom vetoed was SB 7 — colloquially known as the No Robo Bosses Act — which, among other things, would have required employers to provide a written notice to employees when using an automated decision-making system for employment decisions.

The governor also struck down laws that would have: prohibited companion chatbots capable of engaging in certain harmful behaviors from being made available to children (AB 1064); required warning statements on any AI model capable of creating digital replicas (SB 11); required health plans and insurers to indicate in annual reporting the number of denied claims for which AI was used to process, adjudicate, or review (AB 682); mandated that AI-based utilization review decisions must not supplant healthcare provider decision-making or rely solely on group datasets (AB 512); and required data center operators to provide their water suppliers with estimates of expected water use before applying for or renewing business licenses or permits (AB 93).

## Contacts

### [Michael H. Rubin](#)

michael.rubin@lw.com  
+1.415.395.8154  
San Francisco

### [Andrew Gass](#)

andrew.gass@lw.com  
+1.415.395.8806  
San Francisco

### [Ghaith Mahmood](#)

ghaith.mahmood@lw.com  
+1.213.891.8375  
Los Angeles

### [Sy Damle](#)

sy.damle@lw.com  
+1.202.637.3332  
+1.212.906.1659  
Washington, D.C. / New York

### [Fiona Maclean](#)

fiona.maclean@lw.com  
+44.20.7710.1822  
London

*This publication is produced by Latham & Watkins as a news reporting service to clients and other friends. The information contained in this publication should not be construed as legal advice. Should further analysis or explanation of the subject matter be required, please contact the lawyer with whom you normally consult. The invitation to contact is not a solicitation for legal work under the laws of any jurisdiction in which Latham lawyers are not authorized to practice. See our [Attorney Advertising and Terms of Use](#).*

---

## Endnotes

<sup>1</sup> “Catastrophic risk” is defined as a foreseeable and material risk that a large frontier developer’s development, storage, use, or deployment of a foundation frontier model will materially contribute to the death of, or serious injury to, more than 50 people or more than \$1 billion in damage to, or loss of, property arising from a single incident involving a frontier model doing any of the following:

- A. Providing expert-level assistance in the creation or release of a chemical, biological, radiological, or nuclear weapon.

- B. Engaging in conduct with no meaningful human oversight, intervention, or supervision that is either a cyberattack or, if the conduct had been committed by a human, would constitute the crime of murder, assault, extortion, or theft, including theft by false pretense.
- C. Evading the control of its frontier developer or user.

However, the definition explicitly excepts any risk that arises from:

- A. Information that a frontier model outputs that is otherwise publicly accessible in a substantially similar form from a source other than a foundation model.
- B. Lawful activity of the federal government.
- C. Harm caused by a frontier model in combination with other software if the frontier model did not materially contribute to the harm.

<sup>2</sup> In addition to the obligations imposed on frontier developers, SB 53 also requires the California OES to establish a mechanism to be used by both frontier developers and members of the public to report critical safety incidents within specific timeframes. Beginning January 1, 2027, the California OES will publish an annual anonymized and aggregated report describing critical safety incidents that it has received both from developers and the public over the preceding year.

SB 53 also directs the California Government Operations Agency to develop a proposal by January 1, 2027, for CalCompute, a state-backed cloud computing cluster intended to support safe, ethical, equitable, and sustainable AI research and development. The proposal will be developed by a consortium of 14 members that includes representatives of public and private academic research institutions, workforce labor organizations, stakeholder groups, and technology and AI experts, as selected by California's Secretary of Government Operations, Speaker of the Assembly, and Senate Rules Committee.

<sup>3</sup> Companion chatbot" is defined as an AI system with a natural language interface that provides adaptive, human-like responses to user inputs and is capable of meeting a user's social needs, including by exhibiting anthropomorphic features and being able to sustain a relationship across multiple interactions.

"Companion chatbot" does *not* include any of the following:

- (1) A bot that is used only for customer service, a business' operational purposes, productivity and analysis related to source information, internal research, or technical assistance.
- (2) A bot that is a feature of a video game and is limited to replies related to the video game that cannot discuss topics related to mental health, self-harm, sexually explicit conduct, or maintain a dialogue on other topics unrelated to the video game.
- (3) A stand-alone consumer electronic device that functions as a speaker and voice command interface, acts as a voice-activated virtual assistant, and does not sustain a relationship across multiple interactions or generate outputs that are likely to elicit emotional responses in the user.

<sup>4</sup> "Data broker" is defined as a business that knowingly collects and sells to third parties the personal information of a consumer *with whom the business does not have a direct relationship*.

"Data broker" does *not* include any of the following:

- (1) An entity to the extent that it is covered by the federal Fair Credit Reporting Act (15 U.S.C. Sec. 1681 et seq.).
- (2) An entity to the extent that it is covered by the Gramm-Leach-Bliley Act (Public Law 106-102) and implementing regulations.
- (3) An entity to the extent that it is covered by the Insurance Information and Privacy Protection Act (Article 6.6 (commencing with Section 791) of Chapter 1 of Part 2 of Division 1 of the Insurance Code).
- (4) An entity, or a business associate of a covered entity, to the extent their processing of personal information is exempt under Section 1798.146. For purposes of this paragraph, "business associate" and "covered entity" have the same meanings as defined in Section 1798.146.