# California's Safe and Secure Innovation for Frontier Artificial Intelligence Models Act Advances to Adoption in State Legislature

California is currently considering the adoption of a bill that would impose unprecedented new regulations on the development of AI. The bill under consideration is SB 1047, the Safe and Secure Innovation for Frontier Artificial Intelligence Models Act. A full copy of the bill is linked here.

## SB 1047, the Safe and Secure Innovation for Frontier Artificial Intelligence Models Act

The Safe and Secure Innovation for Frontier Artificial Intelligence Models Act or SB 1047 would create a new Frontier Model Division within California's Department of Technology which would have oversight powers over the training of new AI models. Pursuant to SB 1047, developers of AI models would be required to build a so-called kill switch into the AI model and to potentially shut down the model until the Frontier Model Division deems that the AI model is subject to a "limited duty exemption," which would be defined as:

> *a determination. . . . that a developer can provide reasonable assurance that the covered model does not have a hazardous capability, as defined, and will not come close to possessing a hazardous capability when accounting for a reasonable margin for safety and the possibility of posttraining modifications.*

A “covered model” under SB 1047 would be defined to mean an AI model “that was trained using a quantity of computing power greater than 10^26 integer or floating-point operations, and the cost of that quantity of computing power would exceed one hundred million dollars ($100,000,000) if calculating using average market prices of cloud compute as reasonably assessed by the developer at the time of training.”

As currently proposed, “derivative” AI models would be exempt from the new compliance obligations: only “non-derivative” AI models would be subject to the obligations.

Under SB 1047, a  “derivative model” is defined to constitute an artificial intelligence model that is derivative of another AI model, including either ” a modified or unmodified copy of an artificial intelligence model” or “a combination of an artificial intelligence model with another software.  The “derivative model” is defined not to include “an entirely independently trained artificial intelligence model” or an “artificial intelligence model, including one combined with other software, that is fine-tuned using a quantity of computing power greater than 25 percent of the quantity of computing power, measured in integer or floating-point operations, used to train the original model.”

## What constitutes a “hazardous capability” under the proposed legislation?

SB 1047 would define “hazardous capability” to constitute the capability of a covered model to be used in one of the following harms:

- the creation or use of a chemical, biological, radiological, or nuclear weapon in a manner that results in mass casualties
- at least $500 million dollars of damage through cyberattacks on critical infrastructure via a single incident or multiple related incidnts

- at least $500 million dollars of damage by an AI that autonomously engages in conduct that would violate the Penal Code if taken by a human
- bodily harm to another human
- the theft of or harm to property
- other grave threats to public safety and security that are of comparable severity to the harms described above.

Penalties for noncompliance with this legislation would include punitive damages and a civil penalty for a first violation not to exceed ten percent of "the cost of the quantity of computing power used to train the covered model to be calculated using average market prices of cloud compute at the time of training" and 30 percent of the same in case of a second violation. The legislation authorizes joint and several liability against the developers directly where

> *(1) steps were taken in the development of the corporate structure among affiliated entities to purposely and unreasonably limit or avoid liability.*
>
> *(2) The corporate structure of the developer or affiliated entities would frustrate recovery of penalties or injunctive relief under this section.*

If passed, damages could be awarded for violations occurring as of January 1, 2026.

## The reaction to SB 1047 from the Silicon Valley start-up community

As you might expect, the Silicon Valley start-up community is raising concerns about SB 1047.
**Bloomberg** has been reporting on the Silicon Valley reaction, and indicated that that a key concern is that this law is going to "place an impossible burden on developers—and particularly open-source developers, who make their code available for anyone to review and modify— to guaranteed their services aren't misused by bad actors." **Bloomberg** also reported that a general partner at Andreessen Horowitz

indicated that some startup founders are so concerned that they are wondering if they should leave California because of the bill.
**Bloomberg** also reported that the a key point of contention in the startup community is the idea that AI developers are responsible for people who misuse their systems, pointing to Section 230 of the Communications Decency Act of 1996, which has shielded social media companies from liability over content users create on platforms.

Author **Jess Miers** of the Chamber of Progress criticized the legislation on the basis that it would “introduce a high degree of legal uncertainty for developers of new models, making the risks associated with launching new AI technologies prohibitively high.”

The Prinz Law Office will continue following legislative developments relating to SB 1047 as this bill advances.

If you have questions regarding your software company’s potential compliance obligations under SB1047, please schedule a consultation with The Prinz Law Office at this link.