FLOOR ALERT: VOTE "NO" ON SB 1047

The California Chamber of Commerce and above organizations **STRONGLY OPPOSE SB 1047** (Wiener), the Safe and Secure Innovation for Frontier Artificial Intelligence Models Act.

WE SUPPORT SAFE AND SECURE INNOVATION OF AI MODELS. BUT SB 1047 DOES **NOT** ULTIMATELY PROTECT CALIFORNIANS AGAINST UNSAFE AI.

- SB 1047 is fundamentally flawed, and no amount of fine-tuning or clarification can fix what is broken at its core. We should support a national approach to avoid an increasingly fragmenting AI regulatory framework, which is why many of our members have signed on to the White House voluntary commitments to help move toward safe, secure, and transparent development of AI technology. And despite claims that Congress is too dysfunctional, **the federal government IS acting**. In July, Commerce released NIST draft guidance from the U.S. AI Safety Institute to help AI developers evaluate and mitigate risks stemming from generative AI and dual-use foundation models, as required by the 2023 White House Executive Order. **As stated by Speaker Emerita Nancy Pelosi, "the view of many of us in Congress is that SB 1047 is well-intentioned but ill informed."**

SB 1047 RISKS MAKING CALIFORNIA MORE VULNERABLE TO GLOBAL THREATS, UNDERMINING ECONOMIC AND TECHNOLOGICAL INNOVATION.

- While well-intentioned, SB 1047 does precisely what the business community has warned against: regulating the technology itself, threatening California's footing as the home of the world's leading AI companies. By weakening our competitive advantage, it opens the door for other countries to dominate the future of AI—countries which may not play by the same rules that SB 1047 seeks to force upon developers in California.
- Regulatory inconsistency and uncertainty, high compliance costs, and significant liability risks imposed on developers for failing to guarantee against harmful uses of their models by third parties will ultimately have a dramatic and potentially devastating impact on the entire AI ecosystem, discouraging economic and technological innovation. Instead of making Californians safer, the bill would only hamstring businesses from developing the very AI technologies that could protect against dangerous models developed elsewhere.

SB 1047 IS **NOT** LIMITED TO LARGE DEVELOPERS. ITS IMPACT WILL FLOW DOWNSTREAM, DISRUPTING IF NOT DEVASTATING THE ENTIRE AI ECOSYSTEM.

- From AI startups that lose the possibility of building on the latest, more capable AI models, to small businesses using AI to stay competitive in the market, to researchers, independent labs, and academics applying models to solve some of society's biggest challenges, the impact of SB 1047 goes far beyond "Big Tech".

- While recent amendments touched on certain concerns (e.g. penalty of perjury; the timing of training), they fail to address the vast majority of the bill's core concerns:

SB 1047 Imposes Untenable Liability Risks on Developers, Foreclosing Open-Sourcing Large Models.

- Instead of holding bad actors accountable for the harm they cause, SB 1047 holds developers liable for any potential harm caused by a model built off their original model, even if they had no role in building that other model and regardless of the acts of intervening third parties. For instance, a third party could fine tune a model on Chemical, Biological, Radiological, and Nuclear (CBRN) data that the original developer did not.
- Imagine requiring designers or developers of engines of a certain horsepower to guarantee that no one can use or misuse the engine to build a car or other product developed in the future that would be unreasonably dangerous, and then holding them automatically liable for any resulting harm from the end product, even if the engine component was not defective and they had no role in the development of the end product.

SB 1047 Imposes Intrusive and Unreasonable Know Your Customer Obligations and Kill Switch Requirements.

- The bill includes problematic requirements for operators of computing clusters (e.g. data centers or cloud computing companies that provide cloud compute for frontier model training) to collect personally identifiable data from their prospective customers, predict if a prospective customer "intends to utilize the computing cluster to deploy a covered model," and requires the developer to implement a kill switch to enact a full shutdown in the event of an emergency. These obligations violate customer privacy and security creating significant risk that customers will move away from US-based cloud providers.

SB 1047 Creates Regulatory Uncertainty and Suffers from Vagueness, and Overbreadth

- For example, the bill still defines "critical harms" so broadly that it includes not only weapons of mass destruction, but also automated phishing campaigns. As another example, when mandating "reasonable care" in the context of speculative CBRN risks, is it ever reasonable to move forward with a model if a developer cannot totally eliminate the possibility of a critical harm based on future intervening acts of a third party?
- The bill continues to fixate on computing power and cost rather than capability to define covered models. By equating model size to risk, the bill is simultaneously overly broad and too narrow, meaning, critical harms caused by less costly and more efficient AI models can continue to be developed, unchecked.

WHETHER EVALUATING FROM THE STANDPOINT OF SAFETY, TECHNOLOGICAL INNOVATION, OR ECONOMIC VALUE, AS HOME TO 35 OF THE 50 LEADING AI COMPANIES, CALIFORNIA CANNOT AFFORD TO GET THIS WRONG.

WE URGE YOU TO VOTE "NO" ON SB 1047.