

from California Al Students and Faculty

California AI Students and Faculty

Delivered by the UCSB NLP Group Henley Hall, Room 2005 Santa Barbara, CA 93106

August 8, 2024

We the undersigned are academic AI researchers—faculty, postdocs, and graduate students of the University of California at Berkeley, Davis, Los Angeles, Riverside, San Diego, Santa Barbara, and Santa Cruz, of the California Institute of Technology, the University of Southern California and Stanford University—who oppose SB-1047. It will interfere with our academic freedom and ability to conduct our research, in a dubious attempt to mitigate hypothetical impacts of language model advances.

Coverage of the controversy around this bill has centered on corporate factions, "big tech vs little tech," "doomers vs accelerationists," or impacts on the AI industry. We agree that this bill will have broad negative consequences, hamper economic dynamism, and weaken California's position as a global AI hub, in the service of questionable, unscientific, and hypothetical public benefits. However, the purpose of our letter is to offer a researcher-centric perspective in opposition to SB-1047.

As academics, we unequivocally oppose this bill for concern that it may seriously harm both the research and educational objectives of California universities in Al. We call on our representatives to seriously consider these harms when weighing whether to pass this legislation—industry actors are not the only ones who vociferously oppose this bill. Our deep concerns regarding the practical impacts and scientific validity of the bill are as follows:

I. On chilling effects for open-source model releases, to the detriment of our research

We believe requiring "safety auditing" and "full shutdown" capacities in "frontier models" will hinder open-source and open-weight releases, as proprietary models held and controlled by private entities can most easily fulfill these stringent requirements. We are concerned that requiring costly third party auditors on retainer and timely reports of every covered model trained using (as of now undefined) safety auditing protocols will needlessly place undue costs on developers of open models.

The language around how safety will be demonstrated or audited is underspecified in the current text, reliant on hypothetical, to-be-specified tests which currently do not exist, or the opaque assessments currently employed in top private AI research entities. These may not ever be scientifically rigorous. Bearing the potential costs of these audits may be easy to justify for a commercial entity with a profitable product, but we are concerned the same cannot be said for scientifically oriented open releases from commercial entities such as Meta's LLaMA series, or for open models trained by non-profits or consortia of universities. Further, it is unclear how the requirements put forth in the bill will be enforced, and many consequential terms throughout are poorly defined or left to the proposed "Frontier Models Division" to determine.



from California Al Students and Faculty

Considering these onerous restrictions, would-be open-weight model developers may choose to simply build their systems outside of California or the US and release their models under licenses that forbid their use in California to avoid liability. Though proponents of the bill claim it will apply to every entity who does business in California, regardless of where their models are released, the fact that Meta will not be releasing its multimodal LLaMA model in the European Union based on similar regulation while continuing to do business there is an important counterexample [1]. In this scenario private actors without regard for compliance may choose to covertly use the models despite the license restrictions, while academic researchers—bound to comply by the public nature of their work—will be shut out, incentivizing them to either change topics or move to jurisdictions which do not infringe on their academic freedom. Groundbreaking AI research relies on access to open models.

Having access to open models is *crucial* for modern academic AI research. Using open-weight models, academics investigate how models work, how they gain capabilities during training, and how they can be improved and broken [2]. Research on societally consequential issues in language modeling such as copyright infringing outputs [3], fairness and discrimination [4], and secure deployment with private data [4,5] use methods that require open models with documented training procedures—something which private APIs (*application programming interfaces*: closed and opaque paid-access online services) such as OpenAI's or Google's cannot provide. Without this access, such research simply cannot be performed in academia. It is important that this work be conducted *by academic researchers, in the open, for the benefit of the public*, rather than be relegated to trade secrets, trapped behind the confidential walls of private entities based on their proprietary models.

By imposing these stringent restrictions on open LLMs, the bill risks alienating the academic community that relies on these resources, forcing any frontier LM research which does take place to be performed on the few proprietary APIs which can comply. At best, this will just impose potentially prohibitive costs on this research, leaving it only to be performed by the few groups who can afford it. At worst, the LM API providers will have the power to shut out academic researchers performing investigations they don't like or hinder scientific reproducibility by removing access to older model versions. By forcing us to rely on commercial services rather than open-source frameworks, the bill will deprive students opportunities to experiment, learn, and contribute to AI research, without the excessive costs.

II. On the unscientific nature of AI risk forecasting and "capability" assessment

While we are concerned by the negative impacts this bill may have on our research, we are also concerned by its framing which presumes the certainty of hypothetical AI risks. To argue that meaningful risks from AI development—that distinguish them from any other dual-use emerging technology—exist is dubious and ultimately arises from gut opinions, not a scientific basis.

There is *no consensus* in the scientific community on whether and how language models or other "frontier" Al systems may pose a threat to the public [7]. Regarding near-term risks, it is questionable whether a language model can act as an information-generating system that is any more empowering to a nefarious actor than a search engine—any would-be bioweapon developer can just as easily query Google or read textbooks toward "chemical, biological, radiological, or nuclear weapon" (CBRN)



from California Al Students and Faculty

harms invoked in the bill [8]. Regarding long-term risks, we do not believe that "existential" or "catastrophic risks" from AI development are sufficiently evidenced to merit responding in policy at this time. We find it deeply troubling that a law with serious academic and industrial impacts is built on such shaky intellectual ground.

To be clear, these fears over hypothetical existential risks are fundamental drivers for this legislation. Consider two of the four defined "Al safety incidents" a model "autonomously engaging in behavior other than at the request of a user" and enabling "critical harm." "Critical harm" itself means either enabling the creation of CBRN, for which Al's enabling role is dubious, or hypothetical "mass casualty events" or financially costly scenarios arising from autonomous actions taken by an Al system. Credence to the idea of *rogue Al causing mass casualty events* is more in the realm of science fiction than scientific evidence, and because of this is a point of severe contention.

This problematic frame is exemplified in Senator Wiener's response to earlier criticisms of SB-1047 leveled by Y Combinator and Andreessen Horowitz. He notes a point of common desire to "regulate Al for safety" between the bill's promoters and its critics, and that late feedback on the bill is a surprise to him as he posted an outline "in September 2023 for the purpose of soliciting early feedback" [10]. We would like to emphasize that **only those who already believe in existential risks of Al systems**—a group that, while containing some field luminaries, **does not hold a consensus position in the Al research community—would even participate in discussions around safety legislation in its early stages, and this skewed sample gives legislatures a skewed impression of the distribution of Al researcher perspectives on risks**. As we reject the frame that all "risks" alluded to in the bill are certain enough to warrant regulation, it is hard to offer "constructive criticism" to "improve the bill," and we instead call on our representatives to seriously reconsider passing it at all. **Any fact-based debate around this bill must start with the questionably factual nature of Al risk.**

Furthermore, as experts in artificial intelligence, machine learning, and natural language processing, we must stress that *the proposed methods of assessing the "risks" and "capabilities" of models* alluded to in SB-1047 are deeply dubious. Additionally, the proposed use of "capability measurements"—arbitrary and fundamentally flawed benchmarks [9]—is deeply problematic. We do not have a rigorous understanding of how the "capabilities" measured by these tests are related to each other or if they are even meaningful in the real world. Using them as a proxy measure of risk is nonsensical and fundamentally unscientific.

We concur with the August 7th letter to Senator Wiener from US House Representative Zoe Lofgren [10], Ranking Member of the Science Committee. She rightly points out that the law addresses "hypothetical existential risks while largely ignoring meaningful and demonstrable risks such as misinformation, discrimination, nonconsensual deepfakes, environmental impacts, and workforce displacement." Beyond failing to address these harms, this bill *interferes with academic research toward addressing them*—as detailed in Section I—potentially exacerbating them.

III. On the insufficiency of near-term carve outs for open-weight models



from California Al Students and Faculty

Some language in and around the bill has pointed out that no *current* open-source models will be "covered" under the law due to size or training cost [11], that some future carve outs for them may be provided by the "Frontier Models Division," and that some loose phrasing in the bill, such as references to models "under a developer's control" regarding "full shutdown" capabilities, implies open models would be exempt or not impacted. We are not convinced.

It is true that current state-of-the-art open-weight models have parameter counts and training costs orders of magnitude below the limits. However, given the exponential growth of parameter counts and the ever-decreasing cost of compute, there is no reason to expect this situation to hold.

In the absence of iron-clad guarantees protecting open source—which the bill does not provide—we must be wary of the possibility that the consequences described above will come; if not today, in the near future. Low parameter-count models—inherently more usable by independent researchers and small labs due to their lower computational requirements—actually require *more* costly compute to train than larger models of equivalent performance [12], potentially leading to an ironic situation where more-useful-to-release small models are covered while their larger cousins are not.

Thus, we do not believe the proposed amendments intended to mitigate effects on open-source and accessible model releases will mitigate the chilling effects we expect. While a covered model *can* be released under this law, the stringent reporting auditing and requirements under the "Frontier Model Division" that apply to each trained covered model will still needlessly impact our research activities.

IV. Concerns about job placements and career outcomes for our students

Finally, we believe SB-1047 will hinder the aspirations of prospective students interested in Al and computer science. These fields are among the most popular and rapidly evolving on our campuses, yet the bill's constraints might deter new talent from entering these crucial areas. Furthermore, with the tech industry's shift from big corporations to startups—especially noted in the recent trends of 2024—the additional regulatory hurdles could diminish the entrepreneurial spirit by favoring larger, better-resourced companies over emerging innovators. This shift might narrow their career pathways post-graduation. SB-1047 fundamentally interferes with the educational mission of our institutions.

V. Salvagable aspects of the bill

We also concur with Representative Lofgren [10] regarding positive provisions of the bill. We support the establishment of the CalCompute cluster—though its value would be primarily in supporting general academic AI research rather than safe and secure deployment—and see potential value in whistleblower protections, though their utility would primarily be with respect to the real and documented harms rather than the hypothetical AI safety risks. The most "constructive feedback" we have for this bill is to refocus it to these provisions alone and reject the many objectionable ones.

VI. In conclusion



from California Al Students and Faculty

Many important scientific directions are impossible to pursue using commercial APIs—but in the near future, should this law pass, we may have no choice but to use them to investigate frontier models. Without the freedom to explore and push boundaries, the California academic community will fall behind in the global AI race, unable to lead in AI innovation or meaningfully participate in critical discussions on the ethical, safe, and effective uses of AI technologies. The recommended edits by Anthropic do not address any of the fundamental issues listed above.

After the signatures we provide a summary of each of the above numbered citations and how their findings relate to our argument. We hope our explanations will be accessible to non-expert legislators, journalists, and members of the public, and strongly encourage all readers to check them.

As students and faculty of globally leading AI research institutions in California we believe that SB-1047 is fundamentally wrongheaded. It attempts to solve questionably real problems using scientifically unfounded methods, and will be detrimental to educational growth, scientific innovation, and economic development in AI within our California universities, the state of California at large, the United States, and the world. We call on our representatives to listen to all experts and seriously consider our perspective on this matter alongside the more vocal early advocates of the bill. We ask them to consider that early advocates were motivated to engage based on their honestly held (but questionably true) fears of catastrophic AI risks, while we had no reason to engage until it became clear that this bill jeopardizes our scientific and educational mission as it nears passing. We ask that you seriously reconsider passing SB-1047 into law.

The opinions in this letter are solely those of the undersigned and not our institutions.

California faculty

William Wang Mellichamp Professor of Artificial Intelligence University of California, Santa Barbara

Ion Stoica Professor Electrical Engineering and Computer Sciences University of California, Berkeley

Julian McAuley Professor of Computer Science & Engineering University of California, San Diego

Yi Zhang Professor of Computer Science & Engineering University of California, Santa Cruz

Anima Anandkumar



from California Al Students and Faculty

Bren Professor of Computing California Institute of Technology

Taylor Berg-Kirkpatrick Associate Professor Computer Science & Engineering University of California, San Diego

Joseph E. Gonzalez Associate Professor Electrical Engineering and Computer Sciences University of California, Berkeley

Matei Zaharia Associate Professor University of California, Berkeley

Yue Dong Assistant Professor Computer Science & Engineering University of California, Riverside

Muhao Chen Assistant Professor Department of Computer Science University of California, Davis

Xin Eric Wang Assistant Professor Computer Science & Engineering University of California, Santa Cruz

Alane Suhr Assistant Professor Electrical Engineering and Computer Sciences University of California, Berkeley

Prithviraj Ammanabrolu Assistant Professor University of California, San Diego

Uri Manor Assistant Professor



from California Al Students and Faculty

University of California, San Diego

California postdocs and graduate students

Xuandong Zhao Postdoctoral Fellow University of California, Berkeley

Cyril Zakka Postdoctoral Scholar, MD Stanford University

Michael Saxon PhD student and NSF Graduate Fellow University of California, Santa Barbara

Sanjay Subramanian PhD student University of California, Berkeley

lain Weissburg MS Student University of California, Santa Barbara

Jessy Lin PhD Student University of California, Berkeley

Alon Albalak Research Scientist, PhD University of California, Santa Barbara

William Chen
PhD Student
University of California, Berkeley

Isadora White PhD Student University of California, San Diego

Xinyi Wang PhD Candidate University of California, Santa Barbara



from California Al Students and Faculty

Tanishq Mathew Abraham CEO and Research Director, Ph.D. MedARC, Stability AI, University of California, Davis

David Wang Undergraduate Researcher University of California, Santa Barbara

Tanmay Parekh PhD candidate UCLA

Stone Tao PhD Student University of California, San Diego

Reyna Abhyankar CSE PhD Student University of California, San Diego

Deepak Nathani PhD Candidate University of California, Santa Barbara

Daniel Rose MS Student University of California, Santa Barbara

Alfonso Amayuelas PhD Student UC Santa Barbara

Aryaman Arora Ph.D. Student Stanford University

Anikait Singh
PhD Candidate
Stanford University

Zheng Wang MS Student



from California Al Students and Faculty

Stanford University

Isabelle Lee PhD Student University of Southern California

Tejas Srinivasan PhD Candidate University of Southern California

Shushan Arakelyan PhD Candidate University of Southern California, Information Sciences Institute

Hyundong Cho PhD Candidate University of Southern California, Information Sciences Institute

Siddartha Devic PhD Candidate University of Southern California

Jesse Zhang PhD Candidate University of Southern California

Dilara Soylu PhD Student Stanford University

Chunyuan Zheng Undergraduate Researcher UC Berkeley

Concurring academics and researchers from beyond California

Gunnar W. Knutsen Professor, Dr. philos. University of Bergen, Norway

Naomi Saphra Kempner Research fellow Harvard University



from California Al Students and Faculty

Kaiser Sun PhD Candidate Johns Hopkins University

Aaron Gokaslan PhD Student Cornell University

Vardhan Dongre PhD Student University of Illinois Urbana Champaign

Yiran Lawrence Luo PhD Student Arizona State University

Boyuan Chen PhD Candidate MIT

Yongchang Hao PhD Student University of Alberta

Farhan Samir PhD Student University of British Columbia

Blake Harrison Computer Science PhD Student Arizona State University

Alex Lyman PhD Student Brigham Young University

Thom Lake
PhD Student, Principal Scientist
UT Austin

Afra Feyza Akyürek PhD Candidate



from California Al Students and Faculty

Boston University

Carlos E. Jimenez PhD Candidate Princeton University

Daniel Jimenez
ML Research Scientist
Johns Hopkins Applied Physics Laboratory

Keshav Ramji Master's Student University of Pennsylvania

Sat Chidananda Student Arizona State University

Ethan Shen Undergrad Student University of Washington

Jack Hessel Research Scientist, PhD Samaya.ai

Quentin Anthony Head of HPC, PhD EleutherAl

Kevin Ayers Machine Learning Engineer Georgia Tech

Concurring members of industry

Ivan Bercovich Tech Investor ScOp Venture Capital

Chris Lengerich Founder Context Fund



from California Al Students and Faculty

Saurabh Shah ML Engineer Apple

Jim Jones Engineer, UCSB Alum Microsoft

Justin T Chiu Research Scientist, PhD Cohere

Vojta Jina CTO RAINN Inc

Annotated references.

We briefly describe each work referenced in the letter with blurbs motivating either the consequential findings it presented and how it was enabled by open access language models, or a short summary of the paper's role in supporting our argument. All have been published in top international Al venues.

[2] Stella Biderman, Hailey Schoelkopf, Quentin Gregory Anthony, Herbie Bradley, Kyle O'Brien, Eric Hallahan, Mohammad Aflah Khan, Shivanshu Purohit, Usvsn Sai Prashanth, Edward Raff, Aviya Skowron, Lintang Sutawika, Oskar Van Der Wal. Pythia: A Suite for Analyzing Large Language Models Across Training and Scaling. Proceedings of the 40th International Conference on Machine Learning, PMLR 202:2397-2430, 2023. [arxiv.org]

In this work, the authors present a set of open-source, fully documented language models of increasing sizes to facilitate rigorous research on the role that model scaling has on performance on any downstream task. This work has been tremendously empowering for academic researchers—without these open models, only OpenAI, Anthropic, Google, and their ilk would be able to perform this kind of inquiry.

[3] Nicholas Carlini, Daphne Ippolito, Matthew Jagielski, Katherine Lee, Florian Tramer, Chiyuan Zhang. Quantifying Memorization Across Neural Language Models. Proceedings of the International Conference on Learning Representations (ICLR) 2023. [arxiv.org]

In this work, the authors analyze "memorization" of training data in language models that have been trained on documented training data. Work in this vein enables insights into whether and how language models learn to copy and reproduce training data—with consequential implications for copyright and ethical use. While this work was produced at Google, use of non-proprietary (ie., open-source, open-



from California Al Students and Faculty

weight) models is necessary to render this kind of work releasable by private entities, and to make it reproducible. This work was still enabled by open models.

[4] Xisen Jin, Francesco Barbieri, Brendan Kennedy, Aida Mostafazadeh Davani, Leonardo Neves, Xiang Ren. "On Transferability of Bias Mitigation Effects in Language Model Fine-Tuning." *NAACL* 2021 [aclanthology.org]

In this work, the authors investigate and demonstrate fine-tuning techniques to reduce bias against protected groups for hate speech detection and text classification tasks. They show how debiasing fine-tuning for one task can be transferred to another. Fine-tuning is a technique which requires access to a model's weights (ie., open models) in order to be performed reproducibly and inexpensively and is a fundamental method for language model modification after pretraining.

[5] Kandpal, Nikhil, Eric Wallace and Colin Raffel. "Deduplicating Training Data Mitigates Privacy Risks in Language Models." *ArXiv* abs/2202.06539 (2022): n. pag. ICLR 2022 [arxiv.org]

This group of academic researchers, using open language models trained on documented corpora, demonstrate the impact that duplicated examples in training data has on memorization of **private information** in language models. These findings have significant implications—private data such as phone numbers and email addresses are inevitably picked up in the incomprehensibly large datasets language models are trained on, so it is important to investigate how to mitigate the privacy risks this entails. Academic researchers are unbound by the incentives private companies have to not reveal how their systems may leak private information—and academics can only perform this research with open access to models with documented training data.

[6] Kim, Siwon, Sangdoo Yun, Hwaran Lee, Martin Gubri, Sung-Hoon Yoon and Seong Joon Oh. "ProPILE: Probing Privacy Leakage in Large Language Models." *ArXiv* abs/2307.01881 (2023): n. pag. NeurIPS 2023 [openreview.net]

In this work, the authors propose a method to "probe" for personally identifiable information that is memorized by language models, and they verify that their method works using an open language model trained on "the Pile", an open and fully documented training dataset for language modeling. Only with direct access to the training data and a fully transparent model can these important and consequential methods be verified.

[10] Michael Saxon, Ari Holtzman, Peter West, William Yang Wang, Naomi Saphra. "Benchmarks as Microscopes: A Call for Model Metrology." ArXiv abs/2407.16711: COLM 2024. [arxiv.org]

In this work, the authors summarize and survey the broadly agreed-upon notion among academic Al researchers that current benchmarks and metrics which are purported to assess generalized Al capabilities (such as those that form a basis for whether a model is "covered" under SB1047) are



from California Al Students and Faculty

fundamentally broken and not meaningfully predictive of how a model will behave in deployment settings.

[12] Kaplan, Jared, Sam McCandlish, Tom Henighan, Tom B. Brown, Benjamin Chess, Rewon Child, Scott Gray, Alec Radford, Jeff Wu and Dario Amodei. "Scaling Laws for Neural Language Models." ArXiv abs/2001.08361 (2020): n. pag. [arxiv.org]

This (non-peer reviewed, but widely accepted and replicated) technical report from respected OpenAI scientists demonstrates "scaling laws" between compute cost, performance, and model size for LM training. The headline finding is that, counterintuitively, it is actually **less computationally expensive** to train a large LM to some level of performance than a small one, meaning that training an easier-to-use and smaller performant LM would actually be more costly than a large and difficult-to-use one (for academic researchers). This could potentially lead to a situation where an otherwise not-covered model at large and unreleasable sizes becomes covered when trained as a smaller one.

Non-academic references.

[1] Jess Weatherbed. "Meta won't release its multimodal Llama Al model in the EU", The Verge, July 18, 2024. [theverge.com]

Despite doing business in the EU, Meta will be releasing multimodal LLaMA under a license forbidding its use there in light of shifting, unpredictable, and onerous AI safety regulation akin to SB-1047.

[7] Arvind Naraynan and Sayash Kapooor. "Al existential risk probabilities are too unreliable to inform policy." Al Snake Oil, 2024. [aisnakeoil.com]

In this work, these academics convincingly argue that the "p(doom)" (belief that an existentially dangerous AI system will come into existence based on current trends) which are bandied about by AI safety fear merchants is fundamentally unscientific—there is no way to meaningfully assign a probability to the impact of speculative future technology, so such fears should not form the basis of public policy, particularly policies such as SB1047 which have severe externalities.

[8] Mark Scott, Gian Volpicelli, Mohar Chatterjee, Vincent Manancourt, Clothilde Goujard, Brendan Bordelon. "Inside the shadowy global battle to tame the world's most dangerous technology." Politico, March 2024 [politico.eu]

Consider the following excerpt:

In a private hearing between U.S. lawmakers and tech experts in September, [Tristan] Harris, a co-founder of the Center for Humane Technology, a nonprofit, described how his engineers had coerced Meta's latest AI product into committing a terrifying act: the construction of a bioweapon.



from California Al Students and Faculty

Mark Zuckerberg's tech giant favored so-called open-source technology — Al easily accessible to all — with few safeguards against abuse. Such openness, Harris added, would lead to real-world harm, including the spread of Al-generated weapons of mass destruction.

His triumph didn't last long. Zuckerberg, who was also present at the Capitol Hill hearing, quickly whipped out his phone and found the same bioweapon information via a simple Google search. Zuckerberg's counterpunch led to a smattering of laughter from the room. It blunted Harris' accusation that Meta's open-source AI approach was a threat to humanity.

This anecdote is illustrative of our contention that the dangers of "AI technologies" as aids for nefarious actors is questionable—the burden of proof that synthetic text generating systems such as LLMs are more dangerous than search engines with respect to bioweapons and the like is on the claimants—such evidence has **not** been provided yet.

[9] Representative Zoe Lofgren, Letter to State Sen. Scott Wiener, August 7, 2024 [lofgren.house.gov]

[11] Senator Scott Wiener, "Response to inaccurate, inflammatory statements by Y Combinator & a16z regarding Senate Bill 1047" 2024 [safesecureai.org]

From the assumed frame of shared belief in existential AI risks, Senator Wiener points out inaccuracies and misrepresentations in some early statements from Y Combinator and a16z representatives. While we agree that some language in the aforementioned statements, such as sensationalized claims that model makers will be jailed and the like, are inflammatory and unhelpful, we think it is important to point out that the presumed frame of a desire to pass legislation to mitigate questionably valid AI risks which Sen. Wiener references is not shared, with us or presumably with the authors of the original statements. Further, while we may disagree with the authors in specific statements and do not endorse all claims they make about the impacts of SB-1047, we fundamentally share concern toward the consequences of the bill and endorse their efforts to ensure it is not enacted.

Related letters.

We concur with Dr. Fei-Fei Li's op-ed against SB-1047 [fortune.com], which echoes our concerns over the impact of this bill on academia.

Delivered on behalf of all signatories by representatives of the Natural Language Processing Group in the Department of Computer Science of the University of California, Santa Barbara.

UCSB NLP Group Henley Hall, University of California Santa Barbara, California, 93106 https://nlp.cs.ucsb.edu/ Michael Saxon (saxon@ucsb.edu) William Yang Wang (william@cs.ucsb.edu)

Permalink for the letter: nlp.cs.ucsb.edu/uc-sb1047-letter.pdf