August 8, 2024

The Honorable Scott Wiener
California State Senate
1021 O Street
Suite 8620
Sacramento, CA 95814-4900

Dear Senator Wiener,

We, the group of undersigned organizations, Mozilla, EleutherAI, and Hugging Face, are writing to express our concerns regarding SB 1047, the "Safe and Secure Innovation for Frontier Artificial Intelligence Models Act," as currently written. While we support the goals of all draftees to ensure that AI is responsibly developed and deployed, and appreciate the willingness of your team to engage with external parties, we believe that the bill has significant room to be improved so that it does not harm the open-source community.

As you noted in your open letter, "For decades, open sourcing has been a critical driver of innovation and security in the software world,"[1] and we appreciate your commitment to ensure that openness can continue. Open source is already crucial to many of AI's most promising applications in support of important societal goals, helping to solve critical challenges in health[2] and the sciences[3]. Open models reduce the barriers for startups, small businesses, academic institutions, and researchers to utilize AI, making scientific research more accessible and businesses more efficient. By advancing transparency, open models are also crucial to protecting civil and human rights, as well as ensuring safety and security. Researchers, civil society, and regulators can more easily test and assess open models' capabilities, risks, and compliance with the law.[4]

We appreciate that some parts of SB 1047 stand to actively support open science and research. Specifically, we applaud the bill's proposal to create CalCompute to provide access to computational resources necessary for building AI and foster equitable innovation.

We also appreciate that ensuring safe and responsible development and deployment of AI is a shared responsibility.

---

[1] An Open Letter to the AI Community from Senator Scott Wiener, https://safesecureai.org/open-letter.
[2] MedAlpaca: An Open-Source Collection of Medical Conversational AI Models and Training Data, https://arxiv.org/abs/2304.08247.
[3] NVIDIA MegaMolBART: A BART transformer language model trained on molecular SMILES strings, https://catalog.ngc.nvidia.com/orgs/nvidia/teams/clara/models/megamolbart.
[4] Letter from Civil Society and Researchers to NTIA (March 2024) https://cdt.org/wp-content/uploads/2024/03/Civil-Society-Letter-on-Openness-for-NTIA-Process-March-25-2024.pdf

At the same time, responsibility must be allocated in a way that is tailored and proportionate by taking into account the potential abilities of developers and deployers to either cause or mitigate harms while recognizing relevant distinctions in the role and capabilities of different actors. We believe that components of the legislation, as written and amended, will directly harm the research, academic, and small business communities which depend on open-source technology.

We thank your team for their willingness to work with stakeholders and urge you to review several pieces of the legislation which are likely to contribute to such unintended harms, including:

Lack of Clarity and Vague Definitions: In an ecosystem that is evolving as rapidly as AI, definitional specificity and clarity are critical for preventing unintended consequences that may harm the open AI ecosystem and ensuring that all actors have a clear understanding of the expected requirements, assurances, and responsibilities placed on each. We ask that you review the current legislation to ensure that risk management is proportionally distributed across the AI development process as determined by technical feasibility and end user impact.

In particular, we ask that the definition of “Reasonable assurance,” be further defined in consultation with the open-source, academic, and business community, as to exactly what the legislature requires from covered developers as the current definition of “...does not mean full certainty or practical certainty,” is open-ended.

Undue Burdens Placed on Developers: As written, SB 1047 places significant burdens on the developers of advanced AI models, including obligations related to certifying specific outcomes that will be difficult if not impossible to responsibly certify. The developer of an everyday computer program like a word processor cannot reasonably provide assurance that someone will not use their program to draft a ransom note that is then used in a crime, nor is it reasonable for authorities to expect that general purpose tools like open-source AI models should be able to control the actions of their end users without serious harms to fundamental user rights like privacy.

We urge you to consider emerging AI legislative practices and to re-examine how certain obligations within the bill are structured and the likelihood of an individual developer acting in good faith being able to reasonably apply with such obligations. This includes the requirement to identify specific tests and test results that would be sufficient to provide reasonable assurance of not causing or enabling a critical harm, especially as this requirement applies to covered model derivatives.

FMD Oversight of Computing Thresholds: In its current form, the legislation gives the Frontier Model Division (FMD) broad latitude after January 1, 2027, to determine which AI models should be considered covered under the proposed regulation. Given rapid advances in computing, it is likely that in a short time the current threshold set by the legislation will be

surpassed, including by startups, researchers, and academic institutions. As such, these thresholds will quickly become obsolete.

We urge you to create clear statutory requirements for the FMD to ensure that the agency regularly updates the criteria for what is considered to be a covered model in consultation with academia, civil society, the open source community, and businesses. As AI advances and proves not to cause “critical harms," regulators should quickly follow suit to ensure that innovation is not unnecessarily stymied.

Current Definition of Open-Source: As Mozilla research has noted, defining AI open source for foundation models is tricky.[5] However, the current definition of an “Open-source artificial intelligence model,” in the legislation does not include the full spectrum of how researchers and businesses currently release openly available AI models. Today, developers often do so with some legal or technical limitations in place in an effort to make sure their work is used legally and safely. We urge you to broaden the definition and consider working with a body such as the Open Source Initiative to create a legal definition that fully encapsulates the spectrum of openly available AI.

Open-source has been a proven good for the health of society and the modern web, creating significant economic and social benefits.[6] In early 2024, Mozilla and the Columbia Institute of Global Politics brought together over 40 leading scholars and practitioners working on openness and AI – where one of the key findings of the group was that “Openness in AI has the potential to advance key societal goals, including making AI safe and effective, unlocking innovation and competition in the AI market, and bring underserved communities into the AI ecosystem.”[7]

We are strong proponents of effective AI regulation, but we believe that AI risk management and regulatory requirements should be proportionally distributed across the development process based on factors such as technical feasibility and end user impact.

We are committed to working with you to improve SB 1047 and other future legislation. However, as the bill currently stands, we believe that it requires significant changes related to the legislation’s fundamental structure in order to both achieve your stated goals and prevent significant harm to the open-source community.

Sincerely,

Mozilla,

---

[5] Mozilla Foundation: Releasing a new paper on openness and artificial intelligence, https://blog.mozilla.org/en/mozilla/ai/new-framework-for-ai-openness-and-innovation/.
[6] Harvard Business School Strategy Unit Working Paper: The Value of Open Source Software, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4693148.
[7] Mozilla Foundation: Introducing the Columbia Convening on Openness and AI, https://blog.mozilla.org/en/mozilla/ai/introducing-columbia-convening-openness-and-ai/.

EleutherAI,
Hugging Face

cc:
The Honorable Ash Kalra, Chair of the California Assembly Committee on Judiciary
The Honorable Rebecca Bauer-Kahan, Chair of the California Assembly Committee on Privacy and Consumer Protection
The Honorable Buffy Wicks, Chair of the California Assembly Committee on Appropriations
Christine Aurre, Secretary of Legislative Affairs for the Honorable Governor Gavin Newsom
Liz Enea, Consultant, Assembly Republican Caucus