GitHub

88 Colin P Kelly Jr Street,
San Francisco, CA 94107
Tel: 415-448-6673 (main)

April 8, 2025

GitHub Feedback on the Joint California Policy Working Group on AI Frontier Models Draft Report

1. The structure of the Draft Report includes sections about *Context*, *Transparency and Third-Party Risk Assessment*, *Adverse Event Reporting*, and *Scoping*. At a high level, what might you find valuable? What types of questions are you most interested in, and how might you use the report in your work?

GitHub appreciates the opportunity to provide feedback on the Joint California Policy Working Group on AI Frontier Models' Draft Report. We value the report being the result of a multistakeholder process, and its balanced approach to enabling responsible AI-driven innovation. As the world's largest collaborative software development platform and the provider of the leading AI-powered developer tool, GitHub Copilot, we are especially interested in AI policy issues pertaining to open source developers and models, and those that could impact our platform and products. At a high level, Section 3: Transparency is particularly relevant to our developer-focused policy interests.

Section 3: Transparency emphasizes the importance of considering open model weights and recognizes the varied approaches to openness in AI models.

- GitHub is the world's largest code collaboration platform and open source code repository, enabling developers to contribute to and build from a wealth of software code shared under open source licenses. Open source software is a public good, a non-rivalrous and non-excludable knowledge base, enabling use and contribution by professional developers, hobbyists, companies, non-profits, and governments alike. Most software components used to build transformative AI innovations – such as the libraries and code used to collect data, train and test models, and build applications that democratize access to AI tools – are open source and hosted on GitHub. We encourage policymakers to consider how AI functions as a software artifact by integrating code, data, and models into a versionable, maintainable system governed by software development principles.
- GitHub is frequently used to share open-weight models, including the inference code for Llama and DeepSeek models, where developers can fork their own copies of the code for their own

uses. The very definition of what is open source AI, along with questions of the various challenges and opportunities open model weights present–are subject to ever-evolving discussions in the open source developer community. The report noted that while open model weights do not necessarily guarantee heightened transparency, making model weights open enables “deeper inspection into models, which has proven valuable for several forms of scientific research including on safety and security.” This is an important distinction, and is in line with our perspective on the value of sharing open model weights. Open source and open science have been essential to AI development, and widely available model weights, particularly those made available under open source licenses, provide benefits to accountability, innovation, competition, and safety research.

- The report encourages transparency practices that resonate with open source norms such as publishing model documentation, safety evaluations, and allowing third-party assessments. This supports a developer ecosystem where reproducibility and collaborative risk analysis are possible. We also encourage policymakers to consider where potential requirements such as licensing or contractual agreements governing downstream use could impede open source AI development. As referenced in the report, the EU AI Act grants an exemption for open models from the transparency obligations under the AI Act, except where models pose systemic risk. Such risk-proportionate approaches protect collaborative innovation by ensuring that developers can freely share and improve AI models without facing the same regulatory burdens as commercial deployments, thus preserving the vitality of the open source ecosystem.

2. **From your perspective and experience, what key factors do you see affecting California’s path forward in AI governance? Please feel free to provide specific feedback referring to the sections of the draft report.**

From GitHub's perspective, California should focus on clear, practical policies that foster trustworthy AI governance and innovation. This includes applying regulatory interventions as appropriate to different levels of the AI software stack and proportionate to risk. We agree with the draft report’s recommendation that policymakers should center their risk assessment approach on marginal risk, asking if “foundation models present risks that go beyond previous levels of risks that society is accustomed to, such as risks from prior technologies like search engines.” Marginal risk, or the additional risk introduced by a specific change, is a useful framework for evaluating the implications of decisions

such as open sourcing model weights. Regulatory risk assessment should weigh empirical evidence of possible harm against the benefits of widely available model weights, and consider the baseline risks associated with closed, proprietary AI capabilities and the breadth of information available that could be utilized for harmful purposes. Section 5: Scoping proposes setting regulatory thresholds based on criteria like computational resources and financial investment to focus oversight on high-impact AI models. AI capabilities thresholds are a more effective way to govern frontier AI because they connect oversight to what models can actually do, ensuring that regulation is proportionate, adaptive, and focused on real-world risks. GitHub recommends considering how scoping frameworks can be adapted to account for open source models, recognizing the challenges in tracking deployment and impact across various independent projects while ensuring that regulatory thresholds remain relevant and effective.

California should carefully determine when state versus federal governance is most appropriate, promoting a sustainable and inclusive AI ecosystem and avoiding conflict with federal law. For addressing safety and security challenges presented by frontier models, governance is most appropriate at the national level. The U.S. AI Safety Institute is well positioned to both contribute AI safety expertise and coordinate across U.S. agencies and levels of government. That said, California is at the forefront of AI innovation, and has a valuable role to play in accelerating progress while advancing shared commitments to AI safety and security. California is well positioned to invest in research, infrastructure, and education initiatives that advance AI-driven innovation and opportunity.

As the report notes, it is essential that policy be grounded in evidence. One example merits additional nuance, namely 2.5.2 The Importance of Clear Standards: Lessons From Building Codes which states: “Despite these rigorous and extremely prescriptive building standards, homes get built every day. The building code—through significant trial and error—has achieved balance between safety and economic output.” California demonstrates that achieving balance should not be taken for granted, and must be continually re-examined even in a relatively slow moving field such as building standards. Certain standards are well known to have not kept pace with global best practices—for example, permitting single-stair apartments—have contributed to not nearly enough homes being built to meet housing needs. AI policy development needs to be designed to avoid such policy failures by choice.

3. Numerous frontier AI governance-focused groups have been working on frameworks, guidance, and reports aiming to leverage scientific research. For what topics or issues are you observing

challenges in reaching scientific consensus? Do you have recommendations to bridge gaps?

The AI value chain is complex and rapidly evolving, and ambiguity exists on where in the AI stack risk mitigation interventions should be applied. To support the responsible open release of future cutting-edge models, we recommend a research agenda that prioritizes AI evaluations and evidence-based risk mitigations and advancing societal resilience. We recommend supporting research to advance the development of frontier AI capabilities thresholds and on the marginal risks of open release. Furthermore, we recommend research on the benefits of open source AI, including contributions to innovation and economic growth as well as supporting the interpretability, safety, and security of AI models.

4. What could be done individually or collectively to leverage frontier AI for Californians' benefit?

Frontier AI presents major opportunities to enhance software development—automating repetitive tasks, accelerating debugging and code generation, and enabling more people to contribute regardless of experience level. AI-powered developer tools are already transforming software development, accelerating productivity, skilling, scaling, and innovation in software development. AI presents significant opportunities for the American economy and workforce, especially for software development. With AI-powered tools, developers can accelerate coding, streamline code maintenance, and enhance cybersecurity, fostering a more competitive and innovative software ecosystem. AI-powered developer tools lower the barriers to entry into software development, making it easier for developers to learn how to code and create their own software projects. To fully realize these benefits for Californians, it is important to enable developers to share model weights and AI software artifacts openly, while taking a balanced, risk-proportionate approach that avoids excessive regulatory burden on smaller, less resourced contributors and harmonizes with pre-existing AI regulations such as the EU AI Act. California policymakers can support AI development and innovation by investing in open, public-interest infrastructure and ensuring equitable access to AI tools and compute resources for researchers, startups, and independent developers.

Considering that AI innovation depends on a robust open source ecosystem, we encourage approaches that safeguard the open source ecosystem and invest in its sustainability and security to ensure that frontier AI enhances participation in shaping California's digital future.

5. Please feel free to list any published resources you would like to share with the Joint California Policy Working Group on AI Frontier Models.

GitHub. (2024). Octoverse report: the state of generative AI as observed through activity on GitHub. https://github.blog/news-insights/octoverse/octoverse-2024/#the-state-of-generative-ai-in-2024

GitHub. (2024). GitHub Response to NTIA Request for Comment on "Dual-Use Foundation Artificial Intelligence Models With Widely Available Model Weights". https://github.blog/wp-content/uploads/2024/04/NTIA-Submission-2024.pdf

Partnership on AI & GitHub. (2024). Risk Mitigation Strategies for the Open Foundation Model Value Chain: Insights from a Partnership on AI Workshop Co-hosted with GitHub. https://partnershiponai.org/resource/risk-mitigation-strategies-for-the-open-foundation-model-value-chain/

GitHub, Hugging Face, Creative Commons, EleutherAI, LAION, & Open Future. (2023). Supporting Open Source and Open Science in the EU AI Act. https://github.blog/wp-content/uploads/2023/07/Supporting-Open-Source-and-Open-Science-in-the-EU-AI-Act.pdf

Shelley McKinley. *Fortune*. (2023). The EU A.I. Act can get democratic control of artificial intelligence–but only if open-source developers get a seat at the table. https://fortune.com/europe/2023/07/17/eu-ai-act-democratic-control-artificial-intelligence-open-source-developers-tech-politics-shelley-mckinley/

GitHub. (2022). EU AI Act: GitHub position paper. https://github.blog/wp-content/uploads/2023/02/GitHub_Position_Paper-AI_Act.pdf

GitHub shares data https://innovationgraph.github.com/insight-reports which informs research, global indices, and policy monitoring, such as the Stanford AI Index https://hai.stanford.edu/ai-index and the OECD AI Policy Observatory https://oecd.ai/en/github