Y Combinator

March 25, 2024

Dear National Telecommunications and Information Administration,

I am writing on behalf of Y Combinator to provide input on the critical issue of open-weight AI models and their implications for innovation, competition, and national interests. As a key stakeholder deeply engaged in the AI startup ecosystem, we believe it is essential to thoughtfully consider the immense potential benefits of open models while proactively managing associated challenges.

The degree of openness of AI models is a crucial factor shaping the trajectory of this transformative technology. Highly open models, with weights accessible to a broad range of developers, offer unparalleled opportunities to democratize AI capabilities and promote innovation across domains. We have seen firsthand the incredible progress driven by open models, with a growing number of startups harnessing these powerful tools to pioneer groundbreaking applications.

Both open-weight AI models and closed-source models carry with them certain risks and tradeoffs that must be carefully navigated. Open-weight models may have a heightened potential for misuse, but they also allow for democratic contribution and oversight. Closed models afford greater control and may mitigate certain dangers, but exacerbate others, including the risks appurtenant to concentrating power among a few dominant players and weaker defenses against adversarial attack, since the responsibility of identifying any pre-release vulnerabilities, and then subsequently patching those vulnerabilities once discovered, falls solely on the developer – potentially leading to slower fixes or a lack of transparency about the model's security posture. The recent, well-documented issues with Gemini's historical image generation depictions offer a very low-stakes preview of how any deficiencies in closed-source models, which are subject only to internal testing, may only be discovered once they are released into the wild.[1]

We believe the benefits of openness ultimately outweigh the drawbacks. Given the extremely broad user base and use cases of current and future AI models, it is nearly impossible to identify all potential risks prior to launch. Open models foster transparency and accountability by subjecting AI development to wider scrutiny and allow for broader societal input into their

[1] See Google's statement regarding Gemini here: https://twitter.com/Google_Comms/status/1760354549481546035. "We're aware that Gemini is offering inaccuracies in some historical image generation depictions ... We're working to improve these kinds of depictions immediately. Gemini's AI image generation does generate a wide range of people. And that's generally a good thing because people around the world use it. But it's missing the mark here."

development. Open-weight models and the robust open-source communities around them enable independent auditing and research into model behaviors, which then leads to technical interventions (i.e., interventions related to the model's code base/model function/wrappers) that complement regulatory oversight by the government. A balance of technical and regulatory intervention will be a necessary tool for oversight of trustworthy AI models; without technical intervention, given the quick pace of innovation, regulators will be playing a perpetual game of catch-up.

Open models are also essential for unlocking the full potential of AI as a general-purpose technology that can be adapted to countless use cases. They level the playing field, enabling startups and researchers to build on the latest advances. This decentralized innovation is key to maintaining global competitiveness and technological leadership. Imposing strict limits on the openness of model weights at this early stage risks constraining innovation and ceding competitive advantage to nations that embrace openness. Instead, policymakers should aim to proactively shape the ecosystem around open models to maximize benefits and mitigate harms.

To fully realize the benefits of open models while mitigating harms, we believe the role of government should be to provide thoughtful guidance and support rather than unduly restrictive controls. This could entail:

1. Developing clear guidelines and best practices for responsible open model development and deployment, created in consultation with academia, small- and medium-sized technology companies, larger incumbent technology companies, and civil society.
2. Investing in research to better understand and manage potential risks, including work on model interpretability, robustness, and security.
3. Spurring development of tools and frameworks for responsible open model use, such as privacy-preserving techniques, content filters, and monitoring systems for misuse.
4. Leading multi-stakeholder efforts to establish norms and standards around open model development to uphold key values and protect national interests.

Y Combinator stands ready to work with NTIA and all stakeholders to realize the immense promise of open-weight AI models while ensuring this technology develops in alignment with our values. With foresight and proactive stewardship, we can harness open models as an incredible tool to finally chip away at some of the world's most intractable challenges.

Thank you for considering our perspective on this pivotal issue.

Sincerely,

Garry Tan
President and CEO
Y Combinator