Insight

Open-Source AI: The Debate That Could Redefine AI Innovation

ANGELA LUNA | SEPTEMBER 3, 2024

Executive Summary

- A major debate around artificial intelligence (AI) is whether to promote closed or open-source AI; proponents of open-source – AI systems with their components available for further study, use, modification, and sharing – argue they promote AI development, greater transparency, and reduce market concentration, while opponents argue they pose safety risks and put some AI companies at a competitive disadvantage.
- Meanwhile, the California legislature recently passed a bill that, in an attempt to mitigate potential safety risks from advanced AI models, would require large AI models' developers to implement strict safety and security protocols and assume liability of open-source models and their derivatives – though such requirements might discourage AI developers from opening their models.
- As Congress considers the debate between open or closed AI, lawmakers should be aware of the potential pitfalls of premature regulations that could hinder the development of open-source AI models and AI development more generally.

Introduction

A major debate around artificial intelligence (AI) is whether to promote closed or open-source AI. Proponents of open models – AI systems with their components available for further study, use, modification, and sharing – argue they promote AI development, increase transparency, and reduce market concentration. This approach would also allow small players to potentially catch up with AI's advancements without significant investment in research and development (R&D).

Opponents argue open-source AI models pose safety risks and put some AI companies at a competitive disadvantage. As open-source systems become widely available, they could pose safety risks by increasing the chances of bad actors using these systems for harmful purposes including learning how to create bioweapons and carry out cyberattacks. Additionally, some AI developers may lack incentives to make their models more accessible because opening their models could mean exposing proprietary knowledge to others and having their models replicated by competitors.

Meanwhile, California lawmakers recently passed the Safe and Secure Innovation for Frontier Artificial Intelligence Models Act (SB 1047), which, in an effort to mitigate AI's potential harms, could hinder the development of open-source AI. By making developers of AI models responsible for the downstream use or alteration of their models and requiring them to comply with strict safety requirements, the bill could discourage developers from open-sourcing their models, as compliance costs and accountability for any harmful modifications or misuse would rise.

Both closed and open-source AI pose a certain degree of potential risk and benefit for users and AI developers

that federal agencies are evaluating. Given the complexity of open-source AI, it's vital to consider how regulations might influence its different elements. The California bill is likely to have a negative impact on open model developers. Given this, and considering these models are currently driving technological innovation and billions of dollars in investment, federal lawmakers should carefully assess the possible unintended effects of regulation on the innovation of open AI models.

The Open or Closed AI Debate: Concept, Benefits and Disadvantages

In the process of developing AI frameworks, key stakeholders have faced a range of challenges, including the intricacies of open and closed-source AI and the associated benefits and risks. To be considered open source, an AI system needs to have its components available under licenses that provide freedom to study the system, use it for any purpose, modify it to adapt to new needs, and share it with or without modifications. The main objective of opening a technology is to bring collaboration to advance the development of such technology. Yet the open-source AI spectrum – a spectrum that covers which components of the AI system are made public and the level of access granted – is complex. Some foundation models such as Google DeepMind's Flamingo are fully closed, meaning they are available only to the model developer for internal research. Others, such as OpenAI's GPT-4, are limited access, available to the public but allowing only basic interface interaction with the AI model. Still others, such as Meta's Llama 2, are more open, with widely available model components enabling downstream modification and research.

Considering the spectrum of open-source AI models, regulations could impact a variety of different features inherent to the technology. For example, regulators must consider how developers release different stages of the AI systems, the components of the system that are released, and the wide range of stakeholders involved and impacted. Largely unregulated to this point, there are initiatives from startups, researchers, and big tech companies releasing open models such as the AI Alliance which is focused on pioneering open advancements in AI technology. Not all AI companies are inclined to share their models, however. Developers such as Meta and Hugging Face frequently release models openly, while some other models that power popular services are closed, such as OpenAI's ChatGPT and Google's Gemini. While closed developers, whose business models typically rely heavily on their proprietary AI systems, tend to protect their models to maintain their competitive edge in the market, open developers aim to foster collaboration in the field and potentially catch up with AI's advancements. Additionally, open models allow smaller players to build on their work without significant R&D investment.

Yet the question of whether AI should be open or closed has raised numerous debates, not simply over the economic interests of AI developers, but also over other ethical, safety, and innovation implications. Those who advocate for open models argue that such models promote collaboration by allowing developers and researchers from diverse backgrounds to contribute to AI development and ensure transparency by making the components of the models accessible, which is vital for understanding model functionality and addressing ethical concerns. Open models might also reduce the concentration of power among a small number of companies in the technology's development. On the other hand, those in favor of closed models argue that limiting access to AI models improves safety, as keeping source code and operational details confidential helps prevent misuse from bad actors. Closed models also benefit from rigorous quality control, ensuring high performance and reliability. Finally, by keeping their proprietary information closed, developers can protect the exclusivity they have in their AI technology and thus maintain their competitive edge in the market.

Given the complexity of open-source AI and the recent debates, it's vital to consider how regulations might influence different elements of open-source AI to protect the nascent AI industry.

SB 1047's Potential Effect on Open-source AI

The recently passed California AI bill, SB 1047, aims to address AI safety concerns by establishing standards for AI system developers. The bill would introduce AI safety guidelines that enable the detection of high-risk systems before releasing them to the public to prevent "critical harm," such as the creation or use of chemical, biological, radiological, or nuclear weapons, as well as cyberattacks. The bill is controversial, however, as it would hold AI companies liable for derivatives of their models and would require them to submit public statements describing their safety measures. Under SB 1047, individuals that spend less than $10 million fine-tuning a model will not be classified as developers; instead, accountability will remain with the original, larger developer of the model. The bill's regulations target the largest AI models – those costing at least $100 million and requiring 10-times computing power during training. While now only a handful of companies currently have public AI products that meet these criteria, AI advancement is moving at a fast pace, and soon many models could fall under those characteristics. Notably, Meta's CEO Mark Zuckerberg recently said the next generation of Meta's Llama – an open model that acts as a cornerstone for multiple other models – will require 10-times more computing power, which would subject it to SB 1047's provisions.

By introducing liability for modifications of the models and greater compliance costs, the bill would likely discourage large tech firms from investing in open-source efforts and sharing the software code with other developers. Without access to core models, the bill could also hinder the AI startups that would otherwise use the models for new developments and applications. Thus, concerns have been raised by tech industry giants – such as OpenAI, Meta, and Google, as well as the startup Anthropic – that are urging for a veto of the bill, .

Prospects for Future Regulation

California's regulation of AI is likely to influence Congress' debate about the appropriate regulatory approach to address open or closed AI dilemma – and federal AI legislation.

Last year, President Biden's Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence pursued further exploration of open-source AI and tasked the National Telecommunications and Information Administration (NTIA) and other federal agencies to evaluate the risks and benefits open AI systems pose to civil society, geopolitics, and AI development. In response, the NTIA issued a report that largely embraced open-source models, noting their benefits and suggesting that regulation could become necessary in the future. Specifically, it calls for regulators to actively monitor powerful AI model risks and conduct further research and evaluation on the risks and benefits of open and closed AI models.

SB 1047 is likely to have a big influence on the future of open frontier model developers. But considering these models are currently driving technological innovation and billions of dollars in investment, it is crucial for policymakers to explicitly evaluate how AI regulations might unintentionally impact the dynamic innovation landscape surrounding open models.