Insight

Rethinking the Open-source AI Debate

ANGELA LUNA | SEPTEMBER 2, 2026

Executive Summary:

- Open artificial intelligence (AI) models – those that can be downloaded, inspected, and modified – offer greater access and flexibility of use, while lowering costs and barriers to AI innovation compared with closed models; many policymakers, however, favor closed models over open models based on the assumption that they offer greater safety and control.
- As open models – particularly those from Chinese developers – become more capable and widely adopted by U.S. businesses and other organizations, their growing use is raising questions about the U.S.' AI leadership and national security tensions.
- Rather than treating open models as the problem, policymakers should take an evidence-based approach to managing the risks of increasingly capable models, while recognizing the value of both open and closed models in maintaining a diverse and competitive AI stack.

Introduction

Artificial intelligence (AI) models can be released along a spectrum, from closed (or proprietary) models controlled by their developers to fully open-source models whose components are available for download. In between are open-weight models, which make the model weights available but not necessarily other components. Both open-source and open-weight models can be referred to generally as "open" models. While open models offer greater access, flexibility of use and lower costs and barriers to innovation compared with closed models, many policymakers remain concerned that greater openness could make AI systems harder to secure and control.

As open models – particularly those from Chinese developers – become more capable, U.S. businesses, developers, researchers, and government organizations are increasingly using them to build and innovate with AI. Yet this growing adoption is raising new questions about U.S. AI leadership, as greater reliance on Chinese models could affect U.S. competitiveness, as well as national security, given potential risks related to data privacy, government use, and sensitive applications.

Rather than treating open models as the problem, policymakers should take an evidence-based approach to managing the risks of increasingly capable models, while recognizing the value of both open and closed models in maintaining a diverse and competitive AI stack.

Open-source AI and the Regulatory Dilemma

Open source has long been a driver of innovation. The early open-source software movement of the 1980s supported the internet and underlying systems by lowering the cost of software and allowing open sharing of knowledge. Today, AI developers and users are seeking to bring the same benefits to AI by developing open-source foundational models. As previous American Action Forum research reported, AI models can be released along a spectrum from closed to open source.

On one end are closed source, or proprietary, models, which are accessed through consumer applications or Application Programming Interfaces (APIs) that allow businesses to use models hosted on the developer's infrastructure. On the other end are fully open-source models, whose components are available for download, modification, and deployment on users' own infrastructure. Somewhere in between are "open-weight" models, which make the billions of parameters learned during training available for download, while other components, such as training code and data, usually remain unavailable to users. Both open-source and open-weight models can be referred to generally as "open" models. Table 1 shows the model release characteristics, with each approach offering different levels of access, data privacy, cost, customization, and control.

Table 1: The AI Model Release Spectrum

Characteristics	Closed/Proprietary Models	Open-Weight Models	Fully Open-Source
Access	Through app or API; weights unavailable	Weights available for download; subject to license or restrictions	Weights + training code + data information available; subject to license or restrictions
Data Privacy	Data processed by developer	Can deploy locally and keep data within own infrastructure	Can deploy locally and keep data within own infrastructure
Cost	High API or subscription fees	Weights may be free or licensed; compute costs remain	May be free or licensed; compute costs remain
Customization	Limited to developer's tools	Can adapt, inspect and modify	Greater ability to study, adapt, inspect and modify as code and data are available
Developer Control	High	Limited	Limited

Source: Adapted from TechTarget – Attributes of open vs. closed AI explained, and Open source initiative – OSAID 1.0

Because AI models, open or closed, contain powerful capabilities, each end of the spectrum offers its own benefits and risks. Supporters of proprietary models argue that they offer greater safety and control over deployment, while supporters of open-source models argue that openness provides greater access, lowers barriers to entry and costs for businesses, and enables the experimentation needed to foster AI innovation. This, however, is not a new debate among policymakers who have often favored proprietary models over open models based on the assumption that they offer greater safety.

The Growing Open-model Market

Open models have expanded significantly across the AI market. Stanford's AI index report shows that the number of AI-related projects on GitHub – a platform used by developers to share and collaborate on open-source software – grew from 1,549 in 2011 to approximately 5.6 million in 2025, and had a year-over-year growth of 24 percent from 2024 to 2025. Additionally, a report from OpenRouter shows that while proprietary models still dominate usage, open source reached approximately 33 percent of usage by late 2025.

Additionally, because companies find that open AI models are cheaper, these models are

becoming an important part of the AI market. For example, a recent study found that proprietary models cost, on average, six times more than open models. The study also estimates that shifting demand from proprietary to open models could reduce average prices by more than 70 percent, potentially generating $24.8 billion in consumer and businesses savings in 2025.

Open models are also becoming more popular internationally. While U.S. companies such as Meta and Google have been major contributors to open model development, companies from China, the United Kingdom and France are gaining popularity. Notably, China's open-AI models are gaining momentum. Hugging Face (a platform of open-source AI systems) reports that among the most popular open models created in 2025, the majority were either developed in China or built from Chinese models. Alibaba's Qwen family, for example, has more than 113,000 derivative models – new models built or modified from Qwen – on Hugging Face. That's more than Meta and Google combined. Chinese open-weight models are also among the most-used models on OpenRouter, with five Chinese models ranking among the top models by weekly usage.

This trend has accelerated following the release of Chinese open models such as DeepSeek and Kimi K3, as their rapidly improving capabilities have both narrowed the performance gap with U.S. closed models and increased their popularity in the market. A report shows that 80 percent of developers building with open-source tools are using Chinese tools, and this past January, the Alibaba Qwen family of models became the most widely adopted open AI systems in the world.

New Tensions: AI Leadership and National Security

As the capabilities and adoption of Chinese open-AI models continue to grow, the tradeoff is expanding to broader tensions of AI leadership and national security.

Open models – particularly those developed in China – are becoming increasingly capable, leading more developers and businesses to use them to build and innovate with AI. For example, telecom companies such as AT&T are using open models, including some developed in China, to replace proprietary models for specific workloads (which now power about 25 percent of the company's overall AI usage and expect it to reach 80 percent over time). AT&T reports this adoption gives them lower costs, greater control over their data, and more flexibility and choice among AI providers. Additionally, the recent Hugging Face and OpenAI incident – in which an agent powered by OpenAI models escaped its testing environment, gained access to the internet, and compromised parts of Hugging Face's infrastructure – exemplifies the cybersecurity utility these models give to U.S. businesses. Hugging Face reported that while it initially used a proprietary model, the model blocked

the analysis because it triggered safety guardrails. The company later deployed an advanced open-weight model developed by Chinese firm Z.ai, allowing it to conduct the analysis while keeping sensitive data within its infrastructure.

But the same adoption that makes these models valuable also brings tradeoffs. The use of Chinese open models by U.S. companies raises some important questions, including concerns on data privacy, U.S. government and businesses' dependence on Chinese models, and the sensitive applications that these models could enable. Moreover, it raises questions over which models become the foundation of the global AI market. Because open models are increasingly driving AI innovation, the companies and countries that supply them could have greater influence not only in how the technology develops, but also in the standards that shape global AI adoption.

Restricting access to Chinese open models could also bring tradeoffs. Limiting access could reduce the range of models available to U.S. developers, businesses, and academia, hindering their ability to study, develop and integrate AI into their work, while also reducing competition by limiting alternatives to models offered by dominant proprietary developers in the United States. The conversation should therefore not be framed as a choice between closed or open models, but on how to build and strengthen a diverse U.S. AI stack.

Regulatory Outlook

While some policymakers and industry have called for aggressive restriction of open models, these efforts failed because of concerns that these measures may stifle AI innovation.

Even as policymakers remain divided on the mechanisms for domestic open-source regulation, the Trump Administration is considering a strategy to restrict U.S. companies from adopting Chinese open models. Some of the measures include adding open-source Chinese AI labs to the Department of Commerce's "Entity List" – a trade restriction list that identifies foreign companies who act against U.S. national security goals – which would effectively cut off U.S. access to Chinese technology without a license. The administration is also considering issuing government advisories on the threats of Chinese AI labs, and public pressure campaigns aimed at U.S. companies that use Chinese models. Additionally, there is growing speculation that the administration could issue an executive order on open-source AI, which could potentially limit governmental and agency use of various open-source tools.

As policymakers continue to debate how to deal with open-source AI, industry has responded in support of it. More than 20 companies signed a letter warning policymakers about the risks of "premature restrictions" on open models, arguing that those measures would reduce competition and drive innovation abroad.

While the letter does not fully address the concerns associated with open source, the debate highlights the need for a more evidence-based approach to assessing the risks associated with these models. As evidence of the incremental risks posed by open models remains limited – and in some cases speculative – policymakers should weigh the risks against the demonstrated benefits of open source for innovation, access to AI, competition, and data control.

Conclusion

As open models become more capable and widely adopted, market evolution shows that the full spectrum of AI model releases, from closed to open, brings benefits to AI development and adoption, and policymakers should weigh any potential risks against the benefits. Rather than treating open models as a problem, an evidence-based approach to regulating AI could preserve the benefits of a diverse AI stack while addressing the specific risks that come with increasingly capable models.