With Arms Wide Open (or Not): Navigating Open vs. Closed Development of Powerful AI Models
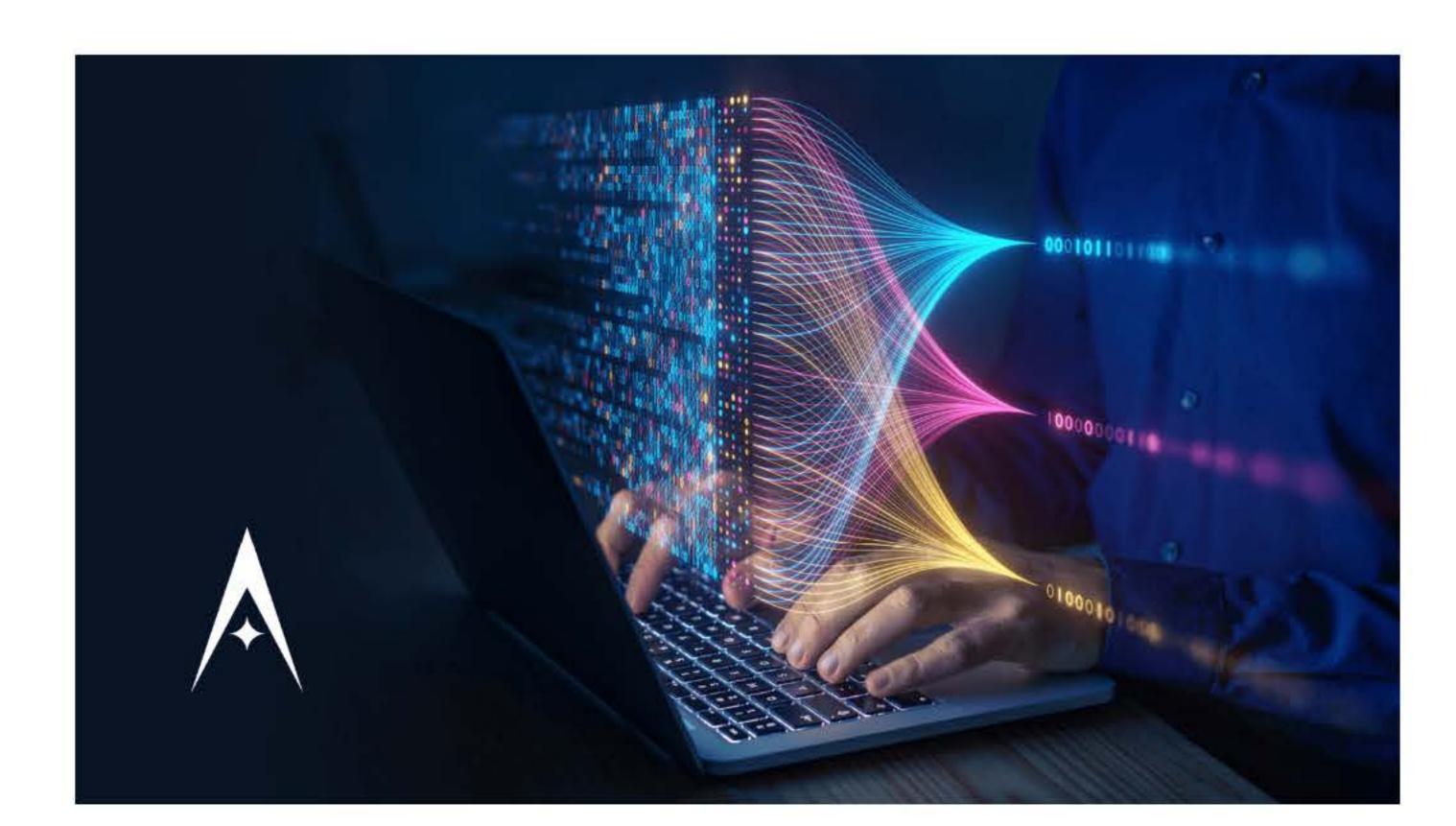

Written by
Adir Mancebo Jr., Ph.D.

Published on
September 1, 2023

As Generative AI rapidly transitions from a technological novelty to an essential tool for many, a pressing debate emerges: Should its development follow an open-source or a closed-source model? This article delves into this critical discussion, weighing the pros and cons of each method, exploring how to responsibly harness the power of AI for the greater good while minimizing risks.

With Arms Wide Open (or Not): Navigating Open vs. Closed Development of Powerful AI Models
By Adir Mancebo Jr., Ph.D.

Generative AI (Gen AI) has quickly transitioned from a technological novelty to an operational imperative, as underscored by McKinsey's latest annual report, "The State of AI in 2023: Generative AI's Breakout Year." Less than a year after the launch of many of these models, a third of the surveyed organizations reported using Gen AI tools regularly. The technology has escalated from being a niche concern of tech teams to a focal point for C-suite executives, with more than a quarter stating that Gen AI is now on their board's agendas [5].

But it is not just within the corporate sphere that Gen AI is making its presence felt. These advanced tools also trickle down to the general public, transforming how we engage with image, text, and audio generation. Just a year ago, such capabilities were restricted to research labs and big tech companies, but now, even everyday users with limited computing power can produce results rivaling human creations [4]. The pace of improvement in these technologies has been amazingly fast—each new iteration of models shows remarkable gains in quality and coherence.

In this context, companies like Google and OpenAI have elected to keep the development of their advanced AI models under wraps, valuing **privacy** over public access. In contrast, companies like Meta and Stability AI advocate for an open-source ethos, prioritizing **transparency**. While the appeal of open source is evident—encouraging greater collaboration and rapid refinement—the potential for misuse by malicious actors is heightened. On the other hand, closed-source models offer more control but often operate in a black box, devoid of public scrutiny.

As we find ourselves at this critical moment, evaluating how these powerful tools are developed is essential. An open-source approach that invites broad collaboration could unlock the potential for tremendous collective benefit. However, a closed development process may seem prudent for mitigating foreseeable risks. With AI reshaping industries, altering workforces, and finding its way into our smartphones and homes, choosing between an open or closed-source developmental approach will have far-reaching implications for companies and society at large.

The Open Source Paradigm

Open-source software is developed collaboratively and made freely available for public use. Unlike proprietary or closed-source software, open-source code is shared transparently so anyone can inspect, modify, or distribute it. The collaborative nature of open-source software—as evidenced by platforms like GitHub and HuggingFace—allows developers to share knowledge and best practices, fostering rapid innovation. Moreover, its transparency ensures trust, as anyone can scrutinize the code for accuracy or malicious intent.

At the forefront of open-source AI development, HuggingFace's CEO Clem Delangue recently argued before the U.S. Congress that by democratizing access to AI capabilities, open-source systems distribute economic gains more broadly, empowering small companies, nonprofits, academics, and other stakeholders to innovate and compete fairly. This transparency and inclusivity fosters accountable development, enabling civil society to audit for issues and counterbalance consolidated corporate power. Still, according to Delangue, open-source AI facilitates solving global challenges through decentralized collaboration that is both ethically open yet responsibly controlled [2].

However, despite its clear advantages, open-source AI carries notable pitfalls that are magnified as the technology becomes more powerful. While open source enables open access, it also allows misuse by ill-intentioned actors, such as spreading misinformation at scale and manipulating others through fake generated content. Moreover, the decentralized nature of open source makes it difficult for institutions to regulate or control these models, posing challenges for governance and accountability. Unfettered openness risks unintended consequences if there are no mechanisms to encourage responsibility.

The Closed Source Argument

In contrast to the open-source ethos, companies like OpenAI and Google have opted for the closed-source route in developing their advanced AI technologies. In fact, OpenAI initially championed an open-source philosophy before transitioning to a closed approach after raising concerns about the misuse of their potent models [7]. It is a fair assessment that, if left unchecked, powerful language models like GPT-4 could become instrumental in various socially harmful activities, from generating misinformation and spam to enabling phishing and fraudulent schemes. By keeping their advanced models behind closed doors, these organizations aim to mitigate such risks.

Going one step further, co-founder and Chief Scientist of OpenAI Ilya Sutskever elaborates on the long-term perspective against open-source AI, arguing that as AI becomes "unbelievably powerful," the ethical obligation to keep it closed becomes stronger [6]. When AI's capability reaches a point where it could be harnessed for large-scale, impactful operations—both good and bad—it raises questions about the responsibility of making such technologies openly available. The underlying concern is that if AI models with vast capabilities are open-source, they could be misappropriated for nefarious ends, causing harm at a scale that could be difficult to contain [6].

However, closed-source development has its drawbacks. While it offers a layer of security against misuse, it also concentrates enormous power and potential in the hands of a few organizations. This lack of public scrutiny could result in biases and flaws in the AI models that go unnoticed and uncorrected. Additionally, the absence of diverse perspectives in the development process could limit the AI's applicability and inclusivity. Thus, while closed-source development may offer a measure of control and risk mitigation, it also raises significant concerns around power concentration, safety of opaque systems, and equitable access to transformative technologies.

Building the Future With Responsibility

As we venture deeper into the advancements in AI, rigid absolutes will only sometimes define the path forward, and instead, ironically require plenty of human input when examining the nuances of open vs. closed sourcing. One possible approach is finding a middle ground, providing free access to proprietary AI models under development for diverse outside researchers and early adopters subject to a safe and controlled environment. This hybrid model could marry the transparency of open source with the safety and control associated with closed source [1].

In this complex and rapidly evolving landscape, transparency, community engagement, and collaborative endeavors are vital, as are privacy, oversight, and social responsibility. While there is no "one size fits all" solution, we must be guided by the principles of Responsible Data Science—upholding and balancing Privacy, Transparency, Veracity, and Fairness—as we develop powerful and impactful systems. Determining how a system can be open or closed-source is not an easy task, as the pros and cons of each are significant. Applying "The Framework for Responsible Data Science Practices" can help organizations thoughtfully define the appropriate balance of open and closed-source elements for a particular AI system [3]. Pursuing a balanced approach, we can aspire to build a world where data and AI serve as instruments for good, enabling progress and innovation without causing harm. The challenge and opportunity before us is not just to advance AI, but to do so responsibly, shaping a better future for humanity.

References:

[1] Asay, M. (2022, July 18). Open source isn't working for AI. InfoWorld.
Article Link

[2] Clem Delangue's testimony before the US Congress. (2023, June 26).
Article Link

[3] Data Science Alliance. (2023). The Framework for Responsible Data Science Practices.
Article Link

[4] Le, D., & Mancebo Junior, A. (2023). Breaking the Technological Fourth Wall: The Democratization of AI.
Article Link

[5] McKinsey & Company. (2023). The state of AI in 2023: Generative AI's breakout year.
Article Link

[6] Open-Source vs. Closed-Source AI. Ilya Sutskever, OpenAI, in conversation with: Ravi Belani, Stanford University. (2023, April 26).
Article Link

[7] Vincent, J. (2023, March 15). OpenAI co-founder on company's past approach to openly sharing research: 'We were wrong.' The Verge.
Aritcle Link