Unraveling Open Source AI

by Melodena Stephens, Mark Esposito, Raed Awamleh, Terence Tse, and Danny Goh

Image Credit | Shahadat Rahman

Defining open source AI and a framework for understanding the ambiguities of the term.

☑ **INSIGHT | FRONTIER**   17 Jun 2024

"Open source" has been a buzzword in the tech community for decades. The term first became popular with software in the 1970s, when operating systems were incompatible and early programming suffered when older systems were replaced (see Richard M. Stallman's (2002) work on free software). However, there has always been ambiguity and speculation about what exactly "open source" means, a debate that recently reopened when Elon Musk sued Open AI in March for reneging on its mission to be open source (Gent, 2024). In this article, we offer a definition of open source AI and a framework for understanding the ambiguities of the term and offer recommendations for the safe and efficient use of open source AI.

Understanding open source AI

Open source AI refers to a combination of what is free in terms of resources of the AI model (API, code, data, hardware, IP), processes (development, testing, feedback, patching), or effects (knowledge, education, products). In general, open-source AI involves the algorithms, code, and data used for training an AI model being made publicly available. The goal in doing so is often to foster collaboration and allow for users, developers, and researchers to build upon and improve the AI model in question (Shrestha et al., 2023). Open source AI is thus a deliberate strategy regarding the access and usage terms of the AI at hand (Fukawa et al., 2021).

Our framework posits that open source AI is not limited to software but can include combinations of software, hardware, data, or knowledge (see Figure 1). It is crucial to note that some projects claim to be "open source" when they only release the neural network model's weights (its pre-trained parameters) while not providing other elements, such as the original dataset or training code (Ramlochan, 2023). Non-profits have worked on developing projects that fully open up the AI model training process, such as the Allen Institute for AI's (2024) **Open Language Model OLMo**.

Even with truly open source software, misconceptions arise. The term does not mean the software is freely available, i.e., the source code (the parts of software copied on computer/device), the code behind this, or the kernel (the part of the software that ties the entire system together) may not be free. In many cases, this misunderstanding is creating

confusion about the actual transparency of AI companies and their altruism (Liesenfeld & Dingemanse, 2024). For example, software that is not free in terms of money but free in terms of usage could be considered open source. For example, **Red Hat Software Inc.,** a publicly traded company, sells subscriptions for Linux-based products, considering that Linux is an open source free software.

Open Source AI

Hardware	Software	Data	Knowledge
Raspberry Pi (except GPU)	Linux AlphaFold (just the source code and public interface)	• Documentation (Raspberry Pi, Signal?) • Training Data (Kaggle data sets, Sigma AI) • Crowd Sourced Data (Waze)	GitHub Waze v3 Kaggle

Figure 1: *Open source AI in terms of hardware, software, data, and knowledge*

Open source AI can allow you to study, use, access, copy/make, modify, distribute, and collaborate, sometimes with strings attached – like a licensing fee, copyright distribution terms, fees for tech support, or other hidden fees (like data storage and access fees once you move to larger data volumes).

Example and Open Source License	Study	Use	Access	Copy/Make	Modify	Distribute	Collaborate
Firefox (The Mozilla Public License)		X		X		X	
Git (GPL-2.0-only)	X	X	X	X (verbatim)		X	X
Linux (GNU General Public License - GPL)		X	X	X	X	X	X
H2O.ai (own legal document)			X				
Open AI (own legal document)	X List of upgrades, but no codes)	X	X		X (via API or fine-tuning some models)		
Tensor Flow (Apache 2.0 License)	X	X	X	X	X	X	X
Signal (GPLv3)		X	X				X
Raspberry Pi (code- GPL; documentation Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA) license)	X	X		(not hardware)	X	X	X

Figure 2: *The Open Source Spectrum*

Using open source AI safely and efficiently

When you choose open source AI projects—for transparency, research collaboration or commercialization—read the fine print. Firstly, investigate who the owner of the project is. The owners of many open source AI projects have a poor track record of keeping promises. When the upkeep of the project becomes expensive, many owners also restrict new model upgrades using a fee structure. It is also crucial to look at how active the community is around the open source project. Are they a dying breed, or are they growing and keeping an eye on each other?

For safety reasons, parts of open source AI code are proprietary. You need to understand the implications of this, especially if you are going to use open source AI as part of a professional or business venture. Software support will also be needed down the line for functioning and cybersecurity. Open source AI can, for example, be embedded with malicious code (see **Harush, 2023)**. If you do not have the necessary cybersecurity expertise yourself, be sure you know how to get it and if you will have to pay for it. If you are building on top of an open source project and planning to commercialize, consider the risks if the project gets corrupted or shifts – how will it impact the functioning of your business? Often, open source means you should also open source derivatives of the project unless you state it specifically, so always read the open source license terms.

Open source AI is often presented as a way to democratize AI development and training. However, open source AI has the same ambiguities and poses the same risks as any other tech trend. Taking the time to understand the variety of open source AI projects out there, how they approach the concept of open source in terms of hardware, software, data, and knowledge, and how to use them safely and efficiently is crucial in order to reap the benefits of this tech while effectively mitigating its risks.

References

Allen Institute for AI. (2024). *Open Language Model: OLMo.* Retrieved May 13, 2024, from **https://allenai.org/olmo**

Fukawa, N., Zhang, Y., & Erevelles, S. (2021). Dynamic capability and open-source strategy in the age of digital transformation. *Journal of Open Innovation: Technology, Market, and Complexity*, *7*(3), Article 175. **https://doi.org/10.3390/joitmc7030175**

Gent, E. (2024, March 25). The tech industry can't agree on what open-source AI means. That's a problem. *MIT Technology Review.* **https://www.technologyreview.com/2024/03/25/1090111/tech-industry-open-source-ai-definition-problem/**

Harush, J. (2023, November 27). The hidden supply chain risks in open-source AI models. *Checkmarx.* **https://checkmarx.com/blog/the-hidden-supply-chain-risks-in-open-source-ai-models/**

Liesenfeld, A., & Dingemanse, M. (2024). Rethinking open source generative AI: Open-washing and the EU AI Act. In *Seventh annual ACM conference on fairness, accountability, and transparency (ACM FAccT 2024)* (pp. 1-14). Association for Computing Machinery. **https://pure.mpg.de/rest/items/item_3588217_2/component/file_3588218/content**

Ramlochan, S. (2023, December 12). *Openness in language models: Open source vs open weights vs restricted weights*. Prompt Engineering & AI Institute. **https://promptengineering.org/llm-open-source-vs-open-weights-vs-restricted-weights/**

Shrestha, Y. R., von Krogh, G., & Feuerriegel, S. (2023). Building open-source AI. *Nature Computational Science*, *3*(11), 908-911. **https://doi.org/10.1038/s43588-023-00540-0**

Stallman, R. M. (2002). *Free software, free society: Selected essays of Richard M. Stallman*. GNU Press.

Melodena Stephens (Follow)

Melodena works on Metaverse governance, AI ethics and sustainability, agile government, and crisis management at a policy and strategy level. She is a member of several IEEE SA Ethics committees, and a co-author of the upcoming book, 'AI Enabled Business: A Smart Decision Kit.'

Mark Esposito (Follow)

Mark Esposito is Professor at Hult Int'l Business School and Harvard University's Division of Continuing Education and works in public policy at the Mohammed Bin Rashid School of Government. He directs the Hult Futures Impact Lab. He co-founded Nexus FrontierTech and the Circular Economy Alliance. He has written over 150 articles and edited/authored 13 books. His next book, "The Great Remobilization" will be published by MIT University Press in the course of 2023.

Raed Awamleh (Follow)

Raed Awamleh is the Dean of the Mohammed Bin Rashid School of Government leading executive education, policy research, and Master programs. Prior to 2015, Raed was Middlesex University's (UK) Pro Vice Chancellor and Dubai Campus Director. He was also the Dean of Academic Affairs at the University of Wollongong (Australia) in Dubai.

Terence Tse (Follow)

Terence Tse is Professor of Finance at Hult International Business School and a co-founder and executive director of Nexus FrontierTech, an AI company. He is also a co-founder of Excellere, a think tank with the goal to help people explore and release their potential through new technologies. He has worked with more than thirty corporate clients and intergovernmental organisations in advisory and training capacities. He has written over 110 articles and three books including The AI Republic: Building the Nexus Between Humans and Intelligent Automation (2019). His next book, The Great Remobilization, will be published by MIT University Press, in the course of 2023.

Danny Goh (Follow)

Danny Goh is a serial entrepreneur and an early stage investor. He is the partner and Commercial Director of Nexus Frontier Tech, an AI advisory business with presence in London, Geneva, Boston, and Tokyo to assist CEOs and board members of different organizations in building innovative businesses that take full advantage of artificial intelligence technology.