Aligning Global Ethics on Generative AI Usage

The rapid spread of Generative AI (GenAI) tools since OpenAI's coup de'tat with ChatGPT in 2022 has brought about debates about ethical governance that echo those held about nearly every previous generation of technical innovation (Rahimi and Abadi, 2023). However, GenAI has a few unique issues, namely: GenAI is powered by data inputs and often relies on upcycling the existing work of others (Fontana, 2025) which makes investing in GenAI a fundamentally ethically fraught endeavour, and, investing in GenAI has also become something of a proxy war for international players with titans like DeepSeek and OpenAI trading blows (George, 2025). These defining concerns drive the urgency of aligning what the ethics of developing and using GenAI ought to be - a task that demands global cooperation, transparency, and adaptive governance.

The internationally distributed reality of AI development complicates ethical oversight not only due to competition but also because of divergent national policies that create enforcement gaps. Farrand et al. highlighted this fragmentation in their analysis of EU and U.S. cybersecurity policies in 2024, noting how conflicting regulations exacerbate risks. Their conclusion that, "harmonized global standards are critical," resonates with Correa et al.'s 2023 observation that abstract ethical discourse often fails to translate into actionable consensus. It seems that some form of international institution for standards and accountability must be stood up in an attempt to keep international players in line. Something modeled after initiatives like the Paris Call for Cyber Trust (Patil, 2023) could bridge jurisdictional divides and ensure ethical concerns are addressed consistently across legal systems while building public trust in GenAI development.

This feels particularly necessary because effective governance requires more than technical aptitude. As Deckard and Fischerkeller et al. wrote in 2023 and 2022 respectively, tech-rooted solutions inevitably fail without diverse perspectives. While sociologists can identify biases in training data, lawyers can navigate liability frameworks, and community advocates can surface potential harms to marginalized groups (Cavelty & Kavanagh, 2019). Employing such multidisciplinary teams within AI firms or the hypothetical central institution would help realize ethical scrutiny as opposed to what any inside-the-box code-based test framework might hope to do. After all, "technocratic solutions fail without diverse epistemic communities," (Fischerkeller et al., 2022).

At the same time technological knowhow and industry participation will remain fundamental alongside these multidisciplinary interventions. Transparency remains a cornerstone of ethics, yet "black box" systems abound in GenAI which harms public trust and complicates legal recourse. Consequently, Tăbușcă wrote in 2018 that this opacity links to unresolved tensions between privacy and security, while Lotrionte stated in their 2018 paper that existing accountability gaps in cyber operations challenges mirror AI's current struggles. Those with technical understanding and expertise will need to work to create explainable AI and clear accountability chains as they participate in public policy discussions (Deckard, 2023). Implementing algorithmic auditing standards - requiring documentation of data sources, decision logic, and error rates - could streamline compliance with emerging regulations like the EU AI Act while shifting industry norms toward defensible design (Goodman and Trehu, 2022).

Finally, static policies cannot keep pace with AI's evolution. In the realm of cybersecurity, dynamic frameworks such as continuous threat intelligence cycles consistently outperform rigid protocols (Alguliyev et al., 2021). Similarly, the global understanding of GenAI ethics must be constantly informed with real-world case studies in order to similarly help AI practitioners adapt to emerging risks. Wlosinski's 2021 observation that "static policies cannot address evolving adversarial tactics" also holds true for GenAI ethics where yesterday's guidelines may not cover today's capabilities. This holds true not just for product capabilities but industry practices in building - the practices in collecting training datasets have been evolving rapidly and demand ethical oversight (Yu et al., 2024).

A final consideration raised is the possibility of a new "AI winter" where the current unchecked optimism in development could lead to systemic failures that evaporate public trust (Correa et al., 2023). History offers sobering lessons about the dangers of this type of bullish building as these cyclical winters reveal how hype can outpace ethical safeguards, leading to disillusionment and financial sector collapses when failures compound with ethical breaches. This is similar to some of the failures observed in recent years with the digital evolution of financial institutions where rapid adoption of technologies without iterative safeguards resulted in large issues like the SVB collapse (Popkova & Gulzat, 2020; Chen, 2024).

"Technological euphoria often precedes systemic collapse," should be a cautionary meditation for GenAI believers (Tzavara & Vassiliadis, 2024). To stay vigilant in light of this, the tech industry should adopt ethical impact assessments that mirror cybersecurity audits, encouraging engineers to weigh long-term robustness against

short-term innovation as part of the software development lifecycle. This shift would not only help ingrain accountability as part of product ownership but also cultivate cultural skepticism toward the magic bullet narratives that dominate AI discourse.

The GenAI revolution demands that engineers, consumers, and other thought leaders move beyond reactive governance. By learning from cybersecurity's successes and failures, fostering global cooperation, and institutionalizing multidisciplinary oversight, there is an opportunity to build GenAI products with sustainability. Without these measures, the industry risks another winter of public backlash and stalled innovation - a fate foreshadowed by history but preventable through thoughtful collaboration.

References

Alguliyev, R.M., Imamverdiyev, Y.N., Mahmudov, R.S. and Aliguliyev, R.M., 2021. Information security as a national security component. *Information Security Journal: A Global Perspective*, *30*(1), pp.1-18.

Chen, H., 2024. An Study on the Causes and Consequences of the SVB Collapse. In *SHS Web of Conferences* (Vol. 188, p. 01018). EDP Sciences.

Corrêa, N.K., Galvão, C., Santos, J.W., Del Pino, C., Pinto, E.P., Barbosa, C., Massmann, D., Mambrini, R., Galvão, L., Terem, E. and de Oliveira, N., 2023. Worldwide AI ethics: A review of 200 guidelines and recommendations for AI governance. *Patterns*, *4*(10).

Deckard, R. (2023). *What are ethics in AI?* [online] BCS, the Chartered Institute for IT. Available at: https://www.bcs.org/articles-opinion-and-research/what-are-ethics-in-ai/.

Farrand, B., Carrapico, H. and Turobov, A., 2024. The new geopolitics of EU cybersecurity: security, economy and sovereignty. *International Affairs*, *100*(6), pp.2379-2397.

Fischerkeller, M.P., Goldman, E.O. and Harknett, R.J., 2022. *Cyber persistence theory: Redefining national security in cyberspace*. Oxford University Press.

Fontana, A.G., 2025. Intellectual property protection in the era of artificial intelligence and the problem of generative platforms. *The Journal of World Intellectual Property*.

George, A.S., 2025. AI supremacy at the price of privacy: Examining the Tech Giants' Race for data dominance. *Partners Universal Innovative Research Publication*, *3*(1), pp.26-43.

Goodman, E.P. and Trehu, J., 2022. Algorithmic auditing: Chasing AI accountability. *Santa Clara High Tech. LJ*, *39*, p.289.

Lotrionte, C., 2018. Reconsidering the consequences for state-sponsored hostile cyber operations under international law. *The Cyber Defense Review*, *3*(2), pp.73-114.

Patil, S. (2023). *The Impact of Globalisation on Cyberterrorism: A Global Perspective Analyses*. [online] TIJER. Available at: https://tijer.org/tijer/papers/TIJER2310055.pdf.

Popkova, E.G., 2020. Digital economy: Complexity and variety vs. rationality.

Rahimi, F. and Abadi, A.T.B., 2023. ChatGPT and publication ethics. *Archives of medical research*, *54*(3), pp.272-274.

Tăbușcă, S.M., 2011. The Internet between Promotion and Infringement of the Fundamental Rights. Freedom vs. Cybercrimes. *Journal of Information Systems and Operations Management*, *5*, p.1.

Tzavara, V. and Vassiliadis, S., 2024. Tracing the evolution of cyber resilience: a historical and conceptual review. *International Journal of Information Security*, *23*(3), pp.1695-1719.

Wlosinski, L.G., 2021. Cyberthreat intelligence as a proactive extension to incident response. *ISACA Journal*, *6*(1), pp.1-7.

Yu, X., Zhang, Z., Niu, F., Hu, X., Xia, X. and Grundy, J., 2024, October. What Makes a High-Quality Training Dataset for Large Language Models: A Practitioners' Perspective. In *Proceedings of the 39th IEEE/ACM International Conference on Automated Software Engineering* (pp. 656-668).