

Strategic Opacity: The Paradox of Open Source AI Governance in DeepSeek and OpenAI

Abstract

Open source narratives have long been associated with promises of broader participation and more distributed oversight. By making code publicly available, companies often claim to enable users to modify and build on systems, even as key decision rights over deployment and governance remain centralized. Our comparative analysis of DeepSeek and OpenAI's licensing agreements reveals a more complex reality. Transparency and control are not opposites; they can coexist in legally intricate ways. DeepSeek's release regime differs across models. We therefore treat DeepSeek's openness as conditional at the ecosystem level, as platform rules and enforcement mechanisms continue to structure access and use. OpenAI, by contrast, withholds model weights and training data and governs access through proprietary interfaces. In both cases, decision rights remain concentrated; what differs is how control is exercised through licensing terms, platform rules, verification, and compliance arrangements. Drawing on Campolo and Crawford's concept of "enchanted determinism," we identify three shifts in AI governance: control moving from algorithms to protocols, the reframing of transparency and control as compatible through "strategic opacity," and growing regulatory misalignment. These findings challenge regulatory approaches that equate code visibility with meaningful transparency and call for governance frameworks that address protocol-level and ecosystem-wide control mechanisms.

Keywords:

AI governance algorithmic transparency control DeepSeek magical determinism OpenAI strategic opacity

Disclosure statement

No potential conflict of interest was reported by the authors.

Notes

1 By "local deployment," we mean that users can download model weights and run the model on their own infrastructure, such as local servers, cloud instances under their control, or institutional computing clusters, rather than accessing the model only through the provider's hosted API or web interface.

2 DeepSeek releases are not uniform. We use V3 to illustrate a split between code license and additional model terms, while later releases such as R1 adopt MIT for weights and shift most constraints to service-level governance.

3 “The source code for DeepSeek is licensed under the permissive MIT license” (Black Duck Citation2025).

4 “The DeepSeek model itself is governed by the DeepSeek license, which does not meet the definition of an open source license” (Black Duck Citation2025). The text of the MIT License says: “The software is provided ‘as is’... no warranty of any kind” (Open Source Initiative Citationn.d.).

5 “Examples include: military applications, generating false or harmful content, violating personal right” (Black Duck Citation2025).

6 “DeepSeek has the right to use technical means to review user behavior ... and take enforcement actions such as suspending accounts” (DeepSeek Citation2025c).

7 “Users must ... clearly indicate AI-generated content ... and compensate DeepSeek for third-party claims” (DeepSeek Citation2025c).

8 The comparison uses snapshots to illustrate governance logics and does not claim uniform licensing across all DeepSeek releases.

9 The text of the MIT License says: “Permission is hereby granted ... to use, copy, modify, merge, publish, distribute ...” (Open Source Initiative Citationn.d.).

10 “The DeepSeek model is not open source ... users must comply with acceptable use policies” (Black Duck Citation2025).

11 “You may not ... reverse engineer, decompile, or discover the source code of the Services.” (OpenAI Citation2024b).

12 The text of the MIT License says: “The above copyright notice and this permission notice shall be included in all copies” (Open Source Initiative Citationn.d.).

13 “DeepSeek reserves the right to suspend accounts for policy violations” (DeepSeek Citation2025b).

14 “All API requests require authentication via API keys” (OpenAI Citation2024a).

15 “You may not use the Services to develop competing AI models” (OpenAI Citation2024b).

16 OpenAI’s archived 2024 Terms state that it uses “both algorithmic and human interventions” to detect and address content that may violate its Terms or Usage Policies, and may take enforcement action, including restricting access to content, features, or accounts (OpenAI Citation2024b).

17 OpenAI’s archived 2024 Terms prohibit users from attempting to reverse engineer, decompile, or discover the source code or underlying components of its services, including models, algorithms, or systems, and also prohibit bypassing rate limits, restrictions, protective measures, or safety mitigations (OpenAI Citation2024b).

18 “DeepSeek may terminate access if users breach terms” (DeepSeek Citation2025b).

19 OpenAI’s archived 2024 Terms state that OpenAI may restrict, suspend, or terminate access if users breach the Terms or Usage Policies, if required for legal compliance, or if use of the services could cause risk or harm to OpenAI, users, or others (OpenAI Citation2024b).

20 The text of the MIT License says: “No requirement to license derivative works under MIT” (Open Source Initiative Citationn.d.).

21 “We may modify API features or discontinue services at any time” (OpenAI Citation2024b).

22 It is clearly stated in the OpenAI’s Business Terms: You may not “use Output (as defined below) to develop any artificial intelligence models that compete with our products or services.” (OpenAI Citation2023).

23 Article 36 of the Data Security Law: “The competent authorities of the PRC are to handle foreign justice or law enforcement institution requests for the provision of data, according to relevant laws and treaties or agreements concluded or participated in by the PRC, or in accordance with the principle of equality and reciprocity. Domestic organizations and individuals must not provide data stored within the mainland territory of the PRC to the justice or law enforcement institutions of foreign countries without the approval of the competent authorities of the PRC” (Standing Committee of the National People’s Congress Citation2021a).

24 Section 103 § 2713 of the CLOUD Act: “A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider’s possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States” (United States Congress Citation2018).