

The Anthropic–Pentagon Dispute: Commercial AI, Autonomy, and the Question of Control

Abhigyan Singh Negi

Introduction

In early 2026, the United States took the unprecedented step of designating a domestic technology company as a national-security ‘Supply Chain Risk’, a classification more commonly associated with foreign entities regarded as security concerns, including China's Huawei.¹ The Department of War (DoW)² imposed the designation after contract negotiations collapsed with Anthropic Public Benefit Corporation, progenitor behind the Claude family of Artificial Intelligence (AI) models. The dispute was not about price or performance. It was about who decides how a powerful AI model may be used in war: the government that buys it, or the company that builds it. Anthropic filed suit alleging violation of its First Amendment right to free expression, and the litigation remains ongoing. The litigation remains ongoing. However, this case is setting a precedent that reaches well beyond Washington. For any state that now utilises commercial frontier AI to run parts of its security infrastructure, especially India, it could be an indication of challenges soon to be faced at home.

How the Dispute Arose

The trigger was Anthropic's desire to impose certain restrictions on the Pentagon's use of Claude. The company refused to allow its models to be used for mass surveillance of Americans or to operate lethal autonomous weapons systems (LAWS) without human control over targeting and firing.³ The Pentagon, led by Defence Secretary Pete Hegseth, took the view that it should be free to use a lawfully procured AI system for any lawful purpose, and that a private contractor had no business setting ethical conditions on national defence.³ Neither side yielded. When the 27 Feb 2026 deadline passed without an agreement, President Trump directed all federal agencies to cease using Anthropic's technology, while Secretary of Defence Pete Hegseth designated the company a supply chain risk and ordered its phased removal from defence-related work over a six-month period.⁴ The order reached beyond the Pentagon's own systems: it required defence contractors and their partners to certify that they did not use Claude in any work for the department. Until then, Anthropic had been the only AI provider cleared to run on classified military networks, and the Pentagon began looking to replace it with models from other competitors.⁵ The dispute unfolded amid heightened military activity and contingency planning associated with the conflict in the Middle East.

The Legal Battle

Anthropic challenged the move on two fronts. On 09 Mar 2026, it filed a civil complaint in the Northern District of California on five counts: that the designation broke the Administrative Procedure Act by skipping the risk assessment, notice and congressional notification the law requires; that it was retaliation for the company's

protected speech about the safety limits of its own technology, in breach of the First Amendment right to free expression; and that the designation and the cancelled contracts denied it due process.⁶ A narrower petition in the District of Columbia Circuit asked that court, which has jurisdiction over the determination, to review the finding itself.⁶ The government, which declined to comment on the litigation, has defended the designation as a legitimate procurement decision for a military that needs unrestricted lawful access to its tools. The courts have differed in their decisions. In late Mar 2026, a federal judge in San Francisco granted a preliminary injunction, describing the attempt to portray the company as a saboteur as an ‘Orwellian notion’, and allowed federal agencies outside the Department of Defence to continue using Claude.⁷ Two weeks later, the District of Columbia Circuit Court refused to suspend the Pentagon’s designation, finding that the balance of harm favoured the government and that Anthropic’s injury was mainly financial. However, they agreed to hear the case on an expedited schedule.⁸

The Underlying Tension

Underlying the controversy, the case is about control of dual-use software. A frontier model has no fixed purpose: the same system that drafts a logistics plan can help choose targets, and the same one that can summarise documents can also sift a population’s communications. When such models sit inside classified systems during an active conflict, for example, the Pentagon kept using Claude through the recent conflict in the Middle East involving the United States and Iran despite this litigation, a government will resist letting the vendor decide what is permissible. That is the force of the Pentagon’s position: a state at war cannot run its targeting or its intelligence on terms set by a private corporate entity.

Anthropic’s limits against LAWS without a human in the loop and mass surveillance of citizens are not eccentric; they track serious and concerning questions that governments themselves have not yet resolved. Using the full coercive power of the state to punish a company for maintaining that position, and to classify it as an adversary alongside Huawei, sets a precedent that could be used against any contractor whose terms an administration finds unacceptable. Such actions also risk undermining the protections guaranteed under the First Amendment. The deeper issue is structural. A handful of private firms now supply the AI systems that states use for both governance and warfare, and the usage policies established by these firms have quietly evolved into a new form of arms-control and surveillance policy, shaped in corporate boardrooms rather than legislatures.

Implications for India

The value of the episode lies not in choosing a side in an American court, but in the questions that it brings to India. India is developing its indigenous military AI ecosystem, ranging from autonomous recognition, and targeting capabilities pursued under the Innovations for Defence Excellence challenges⁹ to domestically developed AI models designed to reduce dependence on foreign systems. The first lesson is that dependence on any foreign frontier model is itself a strategic exposure. A foreign

vendor may impose restrictions on how India employs its systems, a foreign government may deny access or terminate support, and even a domestic supplier can become a critical point of leverage if excessive dependence develops. Plural sourcing and real indigenous capability are the only durable hedges for real sovereignty.

The second lesson is doctrinal. The two issues at the heart of the dispute, autonomy in the use of force and mass surveillance, are precisely the matters India will have to settle in its own law and military doctrine rather than inherit by default from a supplier's terms of service. This risk can be mitigated only by securing a significant controlling stake in, or co-ownership of, the technology and intellectual property underlying the product.

The third lesson concerns the state's treatment of its own technology firms and industrial base. India is trying to develop an indigenous AI technology base of its own, and this case is a reminder that coercion applied to a domestic entity, while temporarily effective, can sabotage the very ecosystem the government is trying to build. A policy framework must be established beforehand to ensure compliance and minimise conflict between the innovators and the end users.

Conclusion

The dispute is unresolved. The two cases are moving on an expedited track, and either side may yet prevail. However, the larger issue has now been brought to light. The verdict may matter less than the fundamental question that the case has brought into the public domain. India's national security cannot be left vulnerable to the demands of any private entity or contractor as a single point of failure. When frontier AI becomes part of how states fight, who holds the controls: the government or the private entity behind the model? India cannot answer that question by waiting to see how an American court rules.

Endnotes

¹ "Anthropic Loses Appeals Court Bid to Temporarily Block Pentagon Blacklisting", *CNBC*, April 8, 2026, accessed 03 May 2026, <https://www.cnbc.com/2026/04/08/anthropic-pentagon-court-ruling-supply-chain-risk.html>

² "President Trump Signs Order to Rename the Defense Department as the Department of War", *NPR*, 04 September 2025, accessed 04 May 2026, <https://www.npr.org/2025/09/04/nx-s1-5529420/trump-department-of-war-department-of-defense>

³ Peter Beck, "Anthropic Sues Defense Department over Supply Chain Risk Designation", *Lawfare*, 09 March 2026, accessed 04 May 2026, <https://www.lawfaremedia.org/article/anthropic-sues-defense-department-over-supply-chain-risk-designation>

⁴ "Anthropic Sues Trump Administration over 'Supply Chain Risk' Order," *CBS News*, 09 March 2026, accessed 03 May 2026, <https://www.aol.com/articles/anthropic-sues-pentagon-over-supply-160451796.html>

⁵ Matt O'Brien, Konstantin Toropin, and David Klepper, "Anthropic Sues Trump Administration Seeking to Undo Supply Chain Risk Designation", *Associated Press*, March 9, 2026, accessed 05 May 2026, <https://www.barchart.com/story/news/644274/anthropic-sues-trump-administration-seeking-to-undo-supply-chain-risk-designation>

⁶ Haim Ravia and Dotan Hammer, "Anthropic Sues Department of Defense over Supply Chain Risk Designation", *Pearl Cohen*, March 26, 2026, accessed 05 May 2026, <https://www.pearlcohen.com/anthropic-sues-department-of-defense-over-supply-chain-risk-designation/>

⁷ Matt O'Brien, Konstantin Toropin, and David Klepper, "US Judge Blocks Pentagon's 'Orwellian Notion' to Label Anthropic a Supply Chain Risk," *Fortune*, March 26, 2026, accessed 05 May 2026, <https://fortune.com/2026/03/26/us-judge-blocks-anthropic-ban-supply-chain-risk-orwellian-notion/>

⁸ Anthropic PBC v. United States Department of War, No. 26-1049 (U.S. Court of Appeals for the District of Columbia Circuit, filed 09 March 2026).

⁹ Innovations for Defence Excellence (iDEX), Ministry of Defence, Government of India, "AI Based Satellite Image Analysis," *Defence India Startup Challenge (DISC) 4 Challenges*, accessed 05 May 2026, <https://idex.gov.in/challenges-cpt/27/>

Abhigyan Singh Negi is a Research Intern at the Centre for Emerging Technologies for Atma Nirbhar Bharat (CETANB) at the United Service Institution of India. He is currently pursuing his bachelor's degree in Electronics and Computer Engineering in Chennai.

Article uploaded on 24-06-2026

Disclaimer: The views expressed are those of the author and do not necessarily represent the views of the organisation that he/she belongs to or of the USI of India.