AI Surveillance: The Panopticon Reimagined

https://doi.org/10.22151/politikon.61.CON7

Hninn Thanlwin THIT
Università di Bologna (University of Bologna)
hninn.business@gmail.com

Abstract

This paper reinterprets Michel Foucault's Panopticon in the context of AI-enabled surveillance, arguing that algorithmic monitoring now disciplines citizens through pervasive, opaque, and normalized forms of control. While such systems pose a direct threat to democratic freedoms, their global diffusion—evident from China's practices in Xinjiang to predictive policing and spyware elsewhere—demands proactive and accountable governance. I contend that coordinated export controls, coupled with NGO-led exposure and strategic litigation, form an essential counter-disciplinary framework. Together, these mechanisms constrain abusive surveillance, strengthen democratic oversight, and enable citizens to resist becoming the docile bodies of an increasingly automated surveillance order.

Keywords: Artificial Intelligence and Democracy; AI Surveillance; Panopticon; Democratic Accountability; Strategic Litigation; Human Rights

Michel Foucault's concept of the Panopticon remains strikingly relevant in the age of AI. In *Discipline and Punish*, Foucault (1975) describes how Bentham's architectural model disciplines inmates through permanent visibility and transforms surveillance into a form of internalized control. Today, AI-driven systems function as digital panopticons: omnipresent, opaque, and capable of shaping citizen behavior without direct coercion. Unlike past prisons, the modern surveillance tower is algorithmic, diffused throughout society, and normalized under the guise of efficiency and security. Within this digital landscape, Foucault's notion of docile bodies, entities molded by systems of power, no longer refers solely to prisoners or workers, but to ourselves: citizens navigating the chilling effects of algorithmic surveillance. Yet, in the pursuit of a more accountable technological order, there must exist mechanisms, or what Foucault might call technologies of power, that redirect this logic of control toward legal and ethical restraint. The combined use of export controls and NGO-led strategic litigation thus functions as a counter-disciplinary framework, resisting the totalizing effects of algorithmic discipline upon our own docile bodies. By reorienting surveillance's internalized discipline into accountability, these instruments offer particularly apt responses to the intangible power of AI-driven surveillance systems.

While certain forms of surveillance can play a legitimate role in safeguarding public safety, such as countering terrorist threats or defending critical infrastructure, unchecked or pervasive monitoring is a clear act of misuse that infringes upon individual rights and civic freedoms. Among the most pressing AI-related threats, surveillance particularly stands out because it directly governs

citizens' behavior and institutional power in an era of digital repression. Other AI threats, such as disinformation, autonomous weapons, or economic displacement, undermine democracy more indirectly by influencing public opinion or social stability. However, none of these challenges possess the same capacity for a strange, continuous, institutionalized control over citizens themselves that only surveillance enables. It is solely surveillance that intangibly but directly suppresses the political freedoms that make democracy function, erodes the checks and balances that sustain it and concentrates power in state or corporate hands. Once entrenched, these systems are exceedingly difficult to dismantle and allow authoritarian practices to persist even after formal leadership changes. In this sense, AI surveillance delivers a precise strike at the very core of democratic governance.

China is a case that exemplifies the profound risks of AI surveillance. In Xinjiang, Beijing has deployed an integrated system of facial recognition, biometric tracking, and AI-driven monitoring to systematically control Uyghur Muslims, contributing to what has been widely recognized as a largely overlooked genocide (Wang 2023). Echoing John Garnaut's observation that Communist Party leaders from Mao Zedong to Xi Jinping have sought to condition citizen behavior through the manipulation of incentives and disincentives (Bishop 2019), Chinese technologies indeed produce an exceptional mechanism of social control through its constant oversight, predictive profiling, and targeted repression (Roth and Wang 2020). In response, Chinese citizens adapt by using encrypted communications, face masks, and low-tech evasive strategies which reveals the pervasive chilling effect on everyday life (Roth and Wang 2020). The most urgent concern lies in how these risks are not confined to authoritarian regimes but are dispersing globally. From the US use of predictive policing and facial-recognition tools disproportionately impacting low-income minority communities to the Pegasus spyware used by various governments stifling journalists, activists, and opposition figures, we have reached a tipping point where our democratic freedoms—at both national and international levels—are increasingly undermined by the normalization of intrusive AI-enabled surveillance (Edwards 2023).

Given the transnational spread of these technologies, addressing the threat requires proactive regulation. While not purely a democratic practice itself, one crucial approach is using coordinated export controls and corporate restrictions. Our nations bear the heavy duty to carefully regulate facial-recognition systems, predictive policing tools, and biometric databases as controlled exports, while enforcing corporate due diligence to prevent indirect complicity in repression. Yet, export controls alone are insufficient: when major powers restrict sales, developing countries and authoritarian-leaning regimes often turn to alternative, less-regulated suppliers.

Taking the case of Bangladesh, even as a parliamentary democracy facing significant development challenges, the government has invested heavily in surveillance infrastructure, spending nearly US $190 million over the past decade despite its limited economic resources and large population relying on subsistence livelihoods (Tech Global Institute 2025). Many of the technologies, one of which is the AI-enabled body-worn cameras planned for the next election in 2026, procured from nations such as China, Israel and the US are capable of intercepting internet traffic, bypassing encryption, and monitoring popular messaging apps (Digibangla.News 2025). This trajectory illustrates how even nominally democratic governments are increasingly adopting sophisticated AI surveillance technologies and assert that, while export restrictions are necessary, they alone cannot fully halt the global spread of surveillance technology.

In this perspective, moreover, the exposure and strategic litigation efforts led by NGOs offer a critical complementary democratic check on the proliferation of AI-enabled surveillance. Civil-society organizations can uncover hidden infrastructures, document human-rights abuses, and initiate legal challenges that hold governments and corporations accountable. A prominent example is Amnesty International's work on the NSO Group and Pegasus spyware. In 2019, Amnesty's legal action revealed how Pegasus had been used by governments to hack journalists, activists, and opposition figures, enabling victims to be unknowingly tracked, eavesdropped on, and spied upon, with their personal data copied (Amnesty International's Security Lab 2024). This revelation prompted international scrutiny of export licenses and led to concrete regulatory and legal responses of blocklist from the United States as well as legal actions from companies such as Apple and Whatsapp to apprehend the abuse of state-sponsored spyware (Amnesty International's Security Lab 2024). Beyond these immediate effects, the exposure raised public awareness about the intrusive potential of AI-enabled surveillance, pressured tech companies to adopt stronger human-rights safeguards, and established legal and normative precedents constraining the misuse of such tools. Although NGOs cannot dismantle all mass-surveillance systems, their exposure, advocacy, and litigation create tangible consequences for governments and corporations and empower citizens to challenge abuses through reshaping accountability norms.

Foucault warned us that power is most dangerous when invisible. AI-enabled surveillance has grown to make this warning a reality by embodying terror through its relentless automation and normalization. By combining proactive export controls with strategic NGO-led exposure and litigation, however, democracies can hence slow the spread of abusive surveillance, empower civil society, and preserve the essential space for dissent. In doing so, even in a world increasingly watched by machines, citizens may refuse the role of docile bodies and instead reclaim agency as active participants in collectively holding power accountable.

References

Amnesty International's Security Lab. 2024. "The Pegasus Project - Amnesty International Security Lab." Amnesty International Security Lab. April 18, 2024. https://securitylab.amnesty.org/case-study-the-pegasus-project/

Bishop, Bill. 2019. "Engineers of the Soul: Ideology in Xi Jinping's China by John Garnaut." *Sinocism* (blog). January 17, 2019. https://sinocism.com/p/engineers-of-the-soul-ideology-in

Digibangla.News. 2025. "Body-Worn Boost: Bangladesh to Equip Police With AI Cameras for Upcoming Election." August 12, 2025. https://digibanglatech.news/156403

Edwards, Ezekiel. 2023. "Predictive Policing Software Is More Accurate at Predicting Policing Than Predicting Crime | ACLU." *American Civil Liberties Union*, February 27, 2023. https://www.aclu.org/news/criminal-law-reform/predictive-policing-software-more-accurate/feed

Foucault, Michel. 1975. *Discipline & Punish: The Birth of the Prison*. Translated by Alan Sheridan. Vintage Books

Roth, Kenneth, and Maya Wang. 2020. "Data Leviathan: China's Burgeoning Surveillance State." *Human Rights Watch*, October 28, 2020. https://www.hrw.org/news/2019/08/16/data-leviathan-chinas-burgeoning-surveillance-state

Tech Global Institute. 2025. "The Digital Police State: Surveillance, Secrecy and State Power in Bangladesh | Tech Global Institute." August 12, 2025. https://techglobalinstitute.com/research/the-digital-police-state/

Wang, Maya. 2023. "China's Algorithms of Repression." *Human Rights Watch*. https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass