DIPLOMACIA
THE WORLD ON TRIAL

AI POWERED TRACKING SYSTEMS: SECURITY AS PROTECTION OR SURVEILLANCE OVERREACH

Jahanvi Singh

IITM Diplomacia Papers

Reviewers: Jashvanth, Sai Nikhil Vukka, Prashant Kumar

May 2, 2026

Abstract

Artificial Intelligence (AI)-powered tracking systems are increasingly being deployed across sectors including public security, transportation, and urban governance, leveraging technologies such as facial recognition, predictive analytics, and real-time data processing to enhance monitoring and response capabilities. Proponents contend that such systems significantly improve public safety, operational efficiency, and crime prevention, while critics raise concerns regarding privacy violations and mass surveillance, raising fundamental questions about where the boundary between protection and control lies. This paper examines the dual nature of AI-powered tracking systems, analyzing their demonstrated benefits in strengthening public security while critically evaluating the ethical, legal, and structural risks of unchecked surveillance expansion. This paper firmly establishes that while AI tracking systems serve as effective and increasingly necessary tools for public protection, their unregulated deployment poses serious ethical and legal challenges that demand immediate and structured policy intervention. Accordingly, this paper concludes by proposing a structured set of policy recommendations designed to balance legitimate security imperatives with the preservation of individual rights and civil liberties.

1 Introduction

AI-powered tracking systems refer to technologies that use artificial intelligence to monitor, identify, and predict the movement or behavior of individuals or objects. These systems integrate tools such as CCTV cameras, GPS tracking, biometric identification, and machine learning algorithms. Governments and organizations increasingly adopt these systems for purposes such as crime prevention, traffic management, and public health monitoring to increase security protection of the citizens. For example, facial recognition systems can identify suspects in real time, while AI-driven analytics can detect unusual patterns that may indicate potential threats.However, the rapid expansion of these technologies has sparked global debate (*India, Surveillance, and the 26/11 Attacks*, 2020). Because while some view them as an essential need for modern security, others see them as unmeasured tools that can enable constant surveillance on the users and erode civil liberties.

2 Critical Analysis

2.1 Security and Efficiency Benefits

AI powered tracking systems work as modern technologies to enhance security and safety. While conventional methods rely heavily on manual human monitoring which remains prone to error and delayed response. In such an era, introduction of AI powered tracking systems becomes an unavoidable necessity. But if we go deeper and thoroughly analyse AI tracking systems, it does not just limit to the physical monitoring of the location only. It is much broader than that.

In urban environments, AI tracking improves public safety by enabling authorities to respond quickly to crimes or emergencies. For instance, smart surveillance systems can detect suspicious and unauthorized activities such as unattended objects or unusual crowd behavior. Whereas in transportation, AI tracking helps manage traffic flow and reduce accidents by monitoring vehicle movements. Furthermore, they are crucial in locating missing persons, tracking stolen goods, and enhancing border security. Their predictive capabilities allow authorities to anticipate potential risks, shifting security from reactive to preventive. A watershed moment in surveillance history was the 2008 Mumbai terror attack on India famously known as the attack of 26/11 (ProPublica, 2019). AI-powered CCTV analysis could have detected suspicious movement patterns in real time. In addition to that, predictive analytics could have identified network communications beforehand. The 26/11 attack exposed a gap in surveillance capability; AI systems specifically addressed this gap by introducing real time tracking systems.Now these systems are in significant use during Ganesh Chaturthi (one of India's largest gathering festivals) where

Mumbai police track the idol using GPS tracking bar codes during the immersion procession. Also, AI cameras were used in the district of Nagpur, Maharashtra for a man-animal conflict resolution to track the location of big cats near the Pench Tiger Reserve (Deccan Chronicle, 2023). Over nearly two decades, this incident prompted a global shift toward smarter surveillance, showing a long trajectory of development.

Moreover, as mentioned above, AI tracking is not limited to this, because along with the live location, it also monitors user behavior — from voice commands to browsing patterns. For instance, when a user expresses interest in purchasing shoes, their device immediately begins displaying targeted advertisements, demonstrating that AI captures and processes behavioral data in real time. This same underlying mechanism, continuous data collection and pattern recognition- powers real-time surveillance tracking systems. When applied in a security context, these identical technologies do not merely recommend products but instead flag suspicious behavioral patterns, track movement across locations, and identify potential threats before they materialize. Therefore, it will not be wrong to say that despite the benefits, the widespread deployment of AI tracking raises concerns about overreach. Continuous monitoring of individuals including the innocent public can lead to a surveillance society where privacy is compromised. Without proper safeguards and restrictions, data collected by these systems can be misused for profiling, discrimination, or political control. In spite of that, this discussion is way more deep and crucial than it actually seems to be.

2.2 Risks of Surveillance and Overreach

Critics argue that AI-powered tracking systems inherently threaten privacy and freedom. Unlike traditional surveillance, AI systems can track individuals continuously and invisibly, often without their consent and can store and use the data later on as happened in 2021, when 'A Pegasus Spyware' developed by NSO group was allegedly used to target Indian politicians and journalists by tracking their phones.

Studies have shown that facial recognition technologies, in particular, have been criticized for inaccuracies and biasness, which may disproportionately affect certain groups. The Gender Shades study (2018) evaluated three major commercial facial recognition algorithms by IBM, Microsoft, and Face++ (Buolamwini & Gebru, 2018). For lighter-skinned males, the error rate was under 1females it rose to 34.7

Additionally, there is a risk of 'function creep', which is a situation where a system is gradually used for purposes beyond its original intent, often without clear consent as also cited in the studies of Author David Lyon. One of broader examples include COVID-19 contact tracing data later being accessed by law enforcement in several countries like

Singapore with TraceTogether App (MIT Technology Review, 2021a, 2021b; NPR, 2021) and Germany with Luca App (US News, 2022; Washington Post, 2022) where the public data stored during the COVID-19 was later used for crime investigation purposes and to contact witnesses respectively.

There are also concerns about data security. Large-scale collection of sensitive personal data increases the risk of breaches, which could expose sensitive information of the citizens, as already happened in 2018 when India's Aadhaar database, one of the world's largest biometric surveillance systems, was compromised when unauthorized agents began selling access to the personal records of over one billion citizens for a nominal fee (Huntress, 2018). This breach exposed a fundamental flaw- that the scale of AI-powered surveillance systems also amplifies the scale of potential harm when security fails. Furthermore, lack of transparency in how AI systems operate makes it difficult to hold authorities accountable leaving no chance for people to take any legal action.

These concerns, while legitimate, identify failures of regulation and implementation rather than fundamental flaws in AI tracking technology itself and are therefore addressable without dismantling the systems entirely. However, it must be acknowledged that regulatory solutions carry their own limitations. Legislation inherently reacts to technological advancement rather than anticipating it. By the time the EU AI Act was passed in 2024 (*EU Artificial Intelligence Act*, 2024), facial recognition technology had already operated without meaningful oversight for nearly a decade. And, oversight mechanisms can fail even when they exist, as demonstrated by India's Aadhaar database breach of 2018 (Huntress, 2018), which occurred despite the Supreme Court of India having established the Right to Privacy as a fundamental right in the landmark Puttaswamy judgement of 2017 (*K.S. Puttaswamy v. Union of India*, 2017), requiring all state surveillance mechanisms to meet strict constitutional scrutiny.

This gap between legal protection and implementation reality does not invalidate regulation but instead argues for stronger enforcement mechanisms, standing regulatory bodies that evolve alongside the technology, and independent oversight with binding rather than advisory authority. The question, therefore, is not whether to regulate AI surveillance but how to build regulatory frameworks robust enough to withstand technological acceleration, institutional failure, and political pressure.

3 Strategic Implications

To balance the benefits of security with the risks of surveillance overreach, the following policy measures must be systematically implemented:

3.1 Clear Legal Frameworks

Governments must enact legally binding legislation that defines the precise boundaries of AI-powered tracking systems, specifying which agencies may deploy them, under what circumstances, and with what level of judicial authorization. The EU AI Act (2024) serves as a working precedent (*EU Artificial Intelligence Act*, 2024).

3.2 Data Protection and Privacy

Strict regulations must govern the collection, storage, and use of surveillance data, both commercially and non-commercially. Legislation must incorporate sunset clauses, legally binding expiry dates beyond which surveillance data must be permanently deleted, preventing the kind of function creep observed when COVID-19 contact tracing data in Singapore and Germany was repurposed for criminal investigations without public consent (MIT Technology Review, 2021a; Washington Post, 2022).

3.3 Transparency and Accountability

Authorities must be legally required to publicly disclose how, where, and how frequently AI surveillance systems are deployed, alongside the results of independent third-party audits conducted every twelve months. The Clearview AI breach of 2020 demonstrated this risk (BBC, 2023; European Data Protection Board, 2022).

3.4 Consent and Public Awareness

Governments must mandate clear, plain-language informed consent disclosures, ensuring citizens are meaningfully aware of how their biometric and behavioral data is collected and accessed.

3.5 Mandatory Accuracy and Anti-Bias Standards

Prior to deployment, all facial recognition and AI tracking systems must meet legislatively defined demographic accuracy benchmarks, demonstrating equal performance across gender, age, and racial groups. The MIT Media Lab Gender Shades study established that error rates for darker-skinned women reached up to 34.7

4 Conclusion

AI-powered tracking systems represent a powerful tool in modern security infrastructure. They offer significant advantages in crime prevention, efficiency, and public safety. However, their potential to enable mass surveillance and infringe on privacy cannot be ignored.

The debate is not simply between security and surveillance but about how to balance the two and how to build regulatory systems powerful enough to withstand technological acceleration, political and institutional pressure. And with appropriate regulations, transparency, and ethical considerations, AI tracking systems can function as instruments of protection rather than tools of overreach. Therefore, rather than abandoning the use of modern technologies, we should adopt and use it with mindfulness, cleverness and awareness. Afterall, humans should be the ones controlling these technologies and not the other way round. So, ultimately, the goal should be to harness the benefits of AI while safeguarding individual freedoms and democratic values.

References

BBC. (2023). *Clearview ai breach report.* Retrieved from https://www.bbc.com/news/technology-67133157

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research*. Retrieved from https://www.media.mit.edu/publications/gender-shades-intersectional-accuracy-disparities-in-commercial-gender-classification

Deccan Chronicle. (2023). *Ai-generated alerts to prevent tiger attacks near pench.* Retrieved from https://www.deccanchronicle.com/nation/ai-generated-alerts-to-prevent-tiger-attacks-near-pench-1943938

Eu artificial intelligence act. (2024). Retrieved from https://artificialintelligenceact.eu/

European Data Protection Board. (2022). *Clearview ai fined by french authority.* Retrieved from https://www.edpb.europa.eu/news/national-news/2022/french-sa-fines-clearview-ai-eur-20-million_en

Huntress. (2018). *Aadhaar data breach analysis.* Retrieved from https://www.huntress.com/threat-library/data-breach/aadhaar-data-breach

India, surveillance, and the 26/11 attacks. (2020). Retrieved from https://verfassungsblog.de/os6-india/

K.s. puttaswamy v. union of india. (2017). Retrieved from https://en.wikipedia.org/wiki/Puttaswamy_v._Union_of_India (Supreme Court of India Judgement)

MIT Media Lab. (2018). *Gender shades project overview.* Retrieved from https://www.media.mit.edu/projects/gender-shades/overview

MIT News. (2018). *Study finds bias in ai systems.* Retrieved from https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212

MIT Technology Review. (2021a). *Singapore says covid-19 contact tracing data accessible to police.* Retrieved from https://www.technologyreview.com/2021/01/05/1015734/singapore-contact-tracing-police-data-covid

MIT Technology Review. (2021b). *Tracetogether and surveillance concerns.* Retrieved from https://www.technologyreview.com/2021/01/11/1016004/singapore-tracetogether-contact-tracing-police

NPR. (2021). *Singapore says contact tracing data can be accessed by police.* Retrieved from https://www.npr.org/sections/coronavirus-live-updates/2021/01/05/953604553/singapore-says-covid-19-contact-tracing-data-can-be-requested-by-police

ProPublica. (2019). *Mumbai attack data: An uncompleted puzzle.* Retrieved from https://www.propublica.org/article/mumbai-attack-data-an-uncompleted-puzzle

US News. (2022). *Contact tracing and privacy concerns.* Retrieved from https://www.usnews.com/news/best-countries/articles/2022-01-19/contact-tracing-biometrics-raise-privacy-concerns-amid-pandemic

Washington Post. (2022). *Germany's luca app and privacy concerns.* Retrieved from https://www.washingtonpost.com/world/2022/01/13/german-covid-contact-tracing-app-luca