Digital Social Science

Innovative

Article

AI Surveillance Technologies and Cybersecurity: Bridging National Security and Privacy Rights

Sujal Chhajed*, Yashasvi Bhalse and Harshwardhan Yadav

National Law Institute University, Kerwa Dam Road, Bhopal-462044, India; yashasvibhalse.ug@nliu.ac.in (Y. B)
harshwardhanyadav.bscllb@nliu.ac.in (H. Y)
* Correspondence: sujalchhajed.bscllb@nliu.ac.in

Abstract: The evolution of national security architectures has begun from reactionary monitoring to proactive, predictive, and "intelligent oversight" in the Indian context. Then, the study examines the impact of deploying advanced surveillance technologies such as facial recognition and behavior analytics on the Smart Cities Mission and their supporting effect on public safety as well as creating significant "regulatory gaps" because of increasing surveillance capabilities that cause fundamental privacy violations. The analysis sheds light on how developing these types of sociotechnical harms may create conditions where algorithmic-biased systems of "digital Jim Crow" continue to reinforce existing inequality based on historical factors but are represented as objective data analysis. Finally, the paper examines how India's continued development trajectory compares to regulators across the globe, specifically contrasting the risk-based regulatory regime of the EU with that of China. China's State centered model, exporting capabilities of surveillance. Ultimately calls for a coordinated strategy, based on the principles of "Industry 5.0", strong legislative oversight and public knowledge, to reconcile demands for national security while maintaining civil rights in a democracy.

Keywords: artificial intelligence surveillance; national security; privacy rights; smart cities mission; predictive policing

1. Introduction

The present design of National Security is moving from a reactive monitoring phase to predicative "intelligent supervision" phase with the introduction of artificial intelligence / machine learning & technology. The ability for State apparatus to predict potential threats before they happen is being rapidly manifested in India through the Smart Cities Project, which has dramatically re-defined urban governance and citizen safety. Over eighty-four thousand (84000+) CCTV Cameras and high technology Traffic Enforcement systems have been installed across the country as part of developing one hundred (100) Smart Cities. This installation of technology has created a datalike environment (Digital Ecosystem). They are able to be "Seen" or Sensed or Secured by citizens in real-time (24/7/365) (Wadhawan 2025). The sheer quantity of installed technology creates many ethical dilemmas or legal ramifications for the citizens who are present within their respective jurisdictions (Aldoseri, Khalifa and Abdel 2024).

As AI (Artificial Intelligence) systems increasingly mediate the relationship between the state (Government) and the individual citizen (or Resident), there now appears to exist a precariously fine balance between collectively establishing strong National Security vs. collectively preserving individual Privacy Rights. The integration of this technology into state and local Public Safety Strategies represents not simply an upgrade to the current technical state of practice, but rather a complete rethinking of the current state of the Social-Technical Landscape. While AI-based surveillance technology has the potential capability to increase the level of Threat Detection and streamline Governance or Government Policies, the potential erosion of civil liberties and increased systemic inequality by way of the use of technology to monitor people's lives creates new types of risks (Reis, Nkechi, and Benedicta et al. 2024). Current research indicates that there are now more sociotechnical harms than ever (a type of harm resulting from the way technology interacts with society); through deploying surveillance methods have resulted in exacerbating existing social vulnerabilities (e.g., representational bias, privacy invasion) as well as breaching privacy rights (Shelby, Shalaleh, and Kathryn et al. 2023).

This situation has been made worse in India where the existing legal framework governing surveillance has struggled to keep pace with the pace of technology (Mirakhori and others 2025).

Citation: Sujal Chhajed, Yashasvi Bhalse and Harshwardhan Yadav. AI Surveillance Technologies and Cybersecurity: Bridging National Security and Privacy Rights. *Digital Social Sciences 2(2),* 10-17.
https://doi.org/10.69971/dss.2.2.2025.43

Copyright: © 2025 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license https://creativecommons.org/licenses/by/4.0/.

Because of this rapid pace of change relative to the application of AI, there are a number of critical regulatory gaps that need to be filled in order to create a sound regulatory framework that balances the benefits of technological innovation with the ethical principles of a democratic society. If there are no checks in place, the state's ability to use existing systems to monitor for potential risks will likely lead to an erosion of the very fundamental rights that the state was created to protect (Jagatheesaperumal, Kashif, and Ala-Al-Fuqaha et al. 2024).

The automation of discrimination is another serious issue related to this subject matter. Over the past few years,[1] legal scholars have been voicing concern over a "Digital Jim Crow" era that utilizes predictive policing algorithms as a means of digitizing and replicating past biases by way of using Objective Data Analysis (Rodriguez 2025). Predictive policing systems use historical crime data to determine what are known as “threat scores” for individual people or communities.[2]

Many of these systems rely on historical crime data that have inherent racial and socioeconomic biases embedded within them from prior policing practices and as such marginalized communities experience a disproportionate amount of policing through the use of these systems.[3] The issue of the inability to audit or hold these predictive policing systems accountable because they rely on secretly owned and operated algorithms, known as the “Blackbox Dilemma,” only adds to the challenges posed by emerging technology. Due to this lack of oversight, many defendants will have significant difficulties challenging the digital evidence relied upon in determining their risk classification.

Secondly, from a geopolitical view, the use of domestic technologies should be placed into context. Diverse regulatory philosophies are defining the current international surveillance/monitoring environment. For example, the EU has enacted the EU AI Act utilizing a risk-based approach by categorizing AI applications by degree of risk demonstrating that they intend to prohibit certain activities from taking place (ex. social scoring) and placing significant limits on the use of biometric identification in a public setting (Santoro and Anonymous 2025). This regulatory approach is very much in contrast to the Chinese Government's approach to usage of AI, which uses AI as a tool for achieving state control through social governance and social stability (ex: Social Credit System) by utilizing AI through facial recognition to monitor individuals and provide a basis for evaluating compliance to societal standards (individual autonomy is secondary to collective security).[4] Furthermore, the research indicates that China is currently 'exporting its surveillance state' by providing facial recognition AI technology to other authoritarian states and weak democracies, thereby reshaping the dynamics of the international norms around privacy and control (Beraja, Andrew, and David et al. 2023).

Autonomous systems and technologies in surveillance have become increasingly important in terms of providing new capabilities. For example, one of the most advanced systems is the U.S. National Reconnaissance Office's (NRO) "Sentient" Program. This system utilizes satellite data to provide real-time predictions about enemy behavior and requires minimal human intervention (future capability) (Scoles 2019). As innovations in this area become available, policymakers will have difficulty balancing the pending technological development's positive attributes, such as the increased use of "Next Generation Solutions" (e.g., cloud-based analytics and edge computing), with protecting us from transforming into a total surveillance state.[5]

2. Overview of AI Surveillance Technologies and Cybersecurity Challenges in the Context of National Security and Privacy Rights

Beginning the development of a nation's security structure from an intelligence-based perspective (AI). AI will establish a national security system that reacts based on monitoring or prediction of future actions (which is referred to as proactive or predictive governing). One such example of this shift in governance towards a more intelligent form of oversight through the intelligence fusion of interconnected data 'points'. In India, this increased intelligence of governance can be seen through the use of the "Smart Cities Mission", which has deployed over 84000 sophisticated surveillance devices capable of not only documenting actions but also interpreting those actions in real time via computer vision and analysis (Scoles 2019) This use of technology for predictive analysis and monitoring of human behaviour (on a global scale) is continuing to grow; for example, in the United States, "Sentient", which functions as the "artificial brain" provides the ability to autonomously assign satellite images for analysis and to use predictive analysis of human behaviour.[6] Yet, this reliance on hyper-connected infrastructure creates a paradox: while these systems enhance physical security, they simultaneously introduce profound cybersecurity vulnerabilities (Tariq, Irfan, and Ali, et al. 2023).

The proliferation of the Internet of Things (IoT) expands the "attack surface" available to malicious actors, creating critical weak points that can compromise sensitive national data and erode public trust. Beyond technical vulnerabilities, the deployment of these technologies generates significant "sociotechnical harms." (Shelby, Shalaleh, and Kathryn et al. 2023). A pressing concern is the rise of predictive policing, which often functions as a "Digital Jim Crow."[7] These algorithmic systems, designed to forecast crime hot spots or individual risk scores, frequently ingest historical data tainted by systemic bias (Rodriguez 2025).

Consequently, they risk automating segregation and digitizing prejudice, disproportionately targeting marginalized communities under the veil of technological objectivity.[8] The "BlackboxDilemma" refers to the lack of transparency in the algorithms that are used to identify people as threats, which can undermine due process for defendants if they are unable to challenge the evidence this algorithm produces against them.[9]

---

1 *Ibid*.

2 *Ibid*.

3 *Ibid*.

4 *Ibid*.

5 Wadhawan (n 1).

6 *Ibid*.

7 *Ibid*.

8 *Ibid*.

9 *Ibid*.

The tension between state security and individual privacy is further complicated by the emergence of generative AI. While these models promise revolutionizing breakthroughs in sectors like healthcare and education, they also possess the capacity to exacerbate socioeconomic inequalities and spread misinformation at an unprecedented scale (Capraro, Austin, and Daron et al. 2023) The dual-use nature of AI means that tools designed for democratization can easily be repurposed for authoritarian control. Research indicates that autocracies are increasingly importing "surveillance state" technologies such as the facial recognition from China, effectively outsourcing the tools of repression to maintain political stability (Beraja, Andrew Kao, and David Yang et al. 2023). China's domestic "Skynet" and "Sharp Eyes" projects demonstrate the apex of this trend, utilizing millions of cameras and big data integration to enforce social norms and suppress dissent, (Wikipedia 2025). a stark contrast to the European Union's risk-based regulatory framework which prioritizes fundamental rights (Santoro and Anonymous 2025).

In India, the ethical and legal systems have not kept up with the rapid acceleration of technology for surveillance. There are many. The fast rate at which surveillance tools/systems are being accepted by the public at large shows that there are many deficiencies in the regulatory framework that allows for these tools/systems to be utilized on the public (Mirakhori and others, 2025).

As the country moves forward in its digital way of living, the challenge will be to ensure that the government's interests in national security do not ultimately infringe upon the civil liberties of its citizens (Reis, Nkechi, Benedicta, and Anthony et al. 2024). Some legal scholars believe that if we fail to develop an efficient and balanced method to audit the algorithms that these tools use for bias and to provide access to them for scrutiny and challenge, any effort to create a "smart" society will undermine the democratic values it was intended to safeguard (Shelby, Shalaleh, and Kathryn et al. 2023).

3. AI Surveillance Technologies Enhancing National Security

The introduction of AI surveillance technology into the fabric of national security fundamentally alters the nature of state power from being based on reactive forms of monitoring (for example, the killing of Osama Bin Laden) to being based on proactive (for example, knowing that Osama Bin Laden is going to do something next week) and predictive forms of providing threat-based management capabilities. These changes are a result of what has been labelled the "Fourth Industrial Revolution" with the primary goal of using sophisticated algorithms and machine learning models to securely maintain public safety and economic stability (Beraja, Andrew, and David et al. 2023).

In the Indian context, this transformation is most visibly operationalized through the Smart Cities Mission, which has integrated digital systems into the core of municipal governance. Recent data indicates that over 84,000 CCTV cameras, alongside thousands of emergency call boxes and public address systems, have been installed across 100 Smart Cities (Wadhawan 2025). These are not passive recording devices; they form an intelligent ecosystem designed to "see, sense, and safeguard" by distinguishing between human and vehicle activity, optimizing traffic flow, and detecting anomalies in real-time.[10]

At the forefront of this technological frontier is the transition from rule-based alerts to complex behavioral analytics. Unlike traditional systems that rely on human operators whose attention spans degrade significantly after just twenty minutes of monitoring AI systems utilize "machine vision" to continuously classify objects and normalize visual data.[11] As these systems learn daily about what "normal" behavior looks like in a given environment, they will be able to autonomously identify and report on unusual behaviors, such as a car driving on the footpath, a crowd of people unexpectedly gathering in a public space, or a fire suddenly erupting, providing a "knock on the shoulder" for human security personnel. This ability to assist with surveillance and reporting is especially useful in "active environments," such as airports and busy metropolitan areas, where the volume of visual data far exceeds the ability of human surveillance personnel to effectively and consistently monitor.[12]

In terms of strategic systems, the United States' Sentient program is perhaps the best example of an AI-enabled intelligence system. Called an "artificial brain", Sentient processes large amounts of data from satellite imagery and other sources of Earth surface information automatically to detect, track and predict what is happening on Earth. When detecting specific signals or images of interest through its "tip-and-cue" feature, it will automatically command other satellites to confirm or track that signal or image to coordinate reconnaissance and track without direct human intervention.[13] This capability to automatically and multiple types of information (for example, optical images and electronic signals) into a single operational view creates a predictive operational picture of what adversary actions will be rather than just reporting them.[14]

The increasing frequency with which these technologies are being used globally helps to show how effective they can be in ensuring that a country remains stable. For example, China has created a "Skynet" system that scans the entire population for criminal activity in less than a second, with great precision, showing how widely and successfully these types of technologies can be used for public safety and crime prevention (Wikipedia 2025). Although there is concern about the geopolitical implications of these types of "surveillance state" technologies, the fundamental technological capabilities associated with this type of technology provide significant strategic advantages in closing the gap between collected data and using data as actionable intelligence for state national security organizations.[15] As India becomes increasingly urbanized, the introduction of "next-generation solutions," such as facial recognition and predictive analytics, will become increasingly critical to the infrastructure of an effective state, allowing the government to respond to anticipated danger or threats in record time and with a great deal of accuracy (Wadhawan 2025).

4. Applications and Effectiveness of AI-Driven Surveillance Systems in Threat Detection and Prevention

---

10 *Ibid*.

11 Artificial intelligence for video surveillance' (*Wikipedia*, 2025) https://en.wikipedia.org/wiki/Artificial_intelligence_for_video_surveillance accessed 17 October 2025.

12 *Ibid*.

13 *Ibid*.

14 *Ibid*.

15 Beraja (n 1).

The ways that modern nation-state security systems operate depend, more and more, on using AI-based video cameras to create pre-emptive monitoring systems, as opposed to basic recording devices. This new technology is illustrated best in urban safety/security where AI-based cameras and predictive analytics are used to expand on what human beings can see and do (Wadhawan 2025). Studies have shown that a human's ability to watch video feeds attentively drops by 95% after 20 minutes of watching, whereas, an AI system can maintain 24/7/365 watchfulness across multiple data streams, continuously (Wikipedia 2025). In India, this capability has been implemented within the Smart Cities Mission program at a large scale. In the next four years (2026), more than 84,000 closed-circuit televisions (CCTV's) will be installed, along with 3,000 public announcement (PA) systems and more advanced traffic enforcement devices like Automatic Number Plate Recognition (ANPR), connected to command centres that enable real-time statistical analysis of irregularities and crowd control.[16]

One of the most significant changes occurring in this area is the transition away from "rules-based" analytics toward "patterns-based" analytics. Older "rules-based" systems required operators to configure all alert types manually; for example, operators had to program an alert when an individual entered a fenced area.[17] Newer "self-learning" algorithms automatically establish a baseline of "normal" Environmental Conditions, so that, after a baseline is established, the systems can identify subtle variations from normal, such as a vehicle driving on a sidewalk or people gathering aggressively, thereby providing an electronic "tap on the shoulder" for security personnel.[18]

This "machine vision" does not merely record pixels but interprets them, classifying objects based on posture, speed, and reflectivity to distinguish between a human intruder and benign motion like wind-blown foliage.[19] Furthermore, these systems enable active deterrence; operators can utilize "talk-down" features to address intruders via loudspeakers immediately upon detection, a tactic proven to significantly reduce theft and vandalism by breaking the perpetrator's sense of anonymity.[20]

At the strategic intelligence level, the United States' "Sentient" program illustrates the apex of these capabilities. Functioning as an "artificial brain," Sentient autonomously fuses multi-modal intelligence ranging from optical imagery to electronic signals to predict adversary actions (McRae and Kaelyn 2026). By using a sophisticated "tip-and-cue" mechanism, one sensor detecting a certain signal will cause all other satellite entities to track and authenticate the sensor's target automatically with no involvement from humans. This creates a "common operational picture" that allows analysts to spend more time making high-level decisions than manipulating data (Aaron and Surya 2023). However, integrating these systems can have some operating friction because they generate so much data that "workslop" (poor quality) AI results require proof from humans to correct, which could overwhelm and fatigue the analyst's brain.

AI's ability to assist with "predictive policing" has also raised a number of questions and criticisms.[21] Imprecise objective tools used for resource allocation through the superiority of objective systems, such as historical crime data sources that generate Heat Lists and Threat Scores, or Intelligent Software, forecast violent offences. However, empirical studies suggest this data are not accurate metrics of Crime Forecasting Accuracy. Case study reviews indicate Geolitica used by Plainfield Police has less than 0.60-0.80% accuracy for Robbery Prediction Rates (only 97/23631 predicted crimes were accurate with respect to Actual Crime Statistics) (Beraja, Andrew, and David et al. 2023). Digital technologies have been in existence for years yet increasing instances of police dependency on Digital Technologies generate digital feedback that enhances targeting of already marginalized populations. This demonstrates systematic discrimination framed by a digital context (i.e., Digital Jim Crow) (Wadhawan 2025). Furthermore, the expansion of such surveillance systems facilitates further expansion of the "attack surface" and, therefore, increases levels of exposure to Cybersecurity Threats whereby sensitive national security information is compromised.[22]

5. Privacy Rights and Ethical Implications in the Indian Context

In the Indian context, the rapid institutionalization of AI surveillance technologies has precipitated a complex ethical crisis, where the imperatives of national security frequently collide with fundamental privacy rights. The deployment of these systems is not incremental but exponential; under the Smart Cities Mission, urban centres are being retrofitted with "intelligent oversight" capabilities, including over 84,000 CCTV cameras and advanced traffic enforcement tools like Automatic Number Plate Recognition (ANPR) (Wadhawan 2025). While these technologies promise to "see, sense, and safeguard" by optimizing public safety and urban governance, they simultaneously vast amounts of sensitive personal data without explicit user consent (B. Sheeja 2025). This creates a pervasive surveillance architecture where citizens are constantly monitored, often unaware of when, where, or how their data is being processed, leading to a tangible erosion of civil liberties.[23]

The tension is evident in India's legal framework which has multiple "regulatory gaps". Technological adoption has increased rapidly due to "next-gen solutions" such as facial recognition and predictive analytics, but robust ethical guidelines and oversight systems have not been developed to the same extent (Mirakhori and others 2024). Legal scholars have indicated that without a complete regulatory infrastructure that reconciles innovation with ethics, there is significant risk of sociotechnical harm. Sociotechnical harm can occur through representational bias of data or by invading individuals' privacy through technology (Shelby, Shalaleh, and Kathryn et al. 2023); this will be particularly damaging to the tenuous nature of trust between the government and its populace

16 Artificial intelligence for video surveillance (*Wikipedia*, 2025) https://en.wikipedia.org/wiki/Artificial_intelligence_for_video_surveillance accessed 17 October 2025.

17 Artificial intelligence for video surveillance (n 2).

18 Sarah Scoles, 'Meet the US's Spy System of the Future — It's Sentient' (*The Verge*, 31 July 2019); see also 'Sentient (Intelligence Analysis System)' (*Wikipedia*, 2025).

19 *Ibid*.

20 *Ibid*.

21 Rodriguez (n 12).

22 *Ibid*.

23 *Ibid*.

.[24] By continuing with its push for a "smart" society, the state may inadvertently undermine democracy through the destruction of fundamental rights of its citizens as a result of advancing digital modernisation (Das 2024).

In addition, AI implementation in law enforcement creates concerns around algorithmic bias which is often referred to as "Digital Jim Crow" (Rodriguez 2025). in the global policy context. Even though many predictive policing applications promote themselves as objective, many of them rely heavily on past crime data which is historically arrived at through systemic bias. When this tainted data is fed into "blackbox" algorithms proprietary systems that are opaque to public auditing it can create feedback loops that disproportionately target marginalized communities.[25] This lack of transparency raises severe due process concerns, as individuals labelled as "high risk" by an algorithm effectively face a digital presumption of guilt without the ability to challenge the underlying evidence.[26] The potential for misuse is amplified by the dual-use nature of these technologies; tools designed for traffic management or crime prevention can easily be repurposed for mass surveillance and social control, echoing the authoritarian "social governance" models seen in neighboring jurisdictions (Beraja, Andrew, and David et al. 2025).

Ethical dualism extends to safety (public) and significant areas like health care, as an illustration of the larger privacy issue: making AI-driven precise medicine and clinical decision support systems highly beneficial for public health at the same time as introducing a serious offence to data privacy and bias in health care treatment outcomes by virtue of utilising an Internet connected to the Internet of Things (IoMT), creating a vulnerability that if there is no rigorous protection from information access to these systems (Varnosfaderani and Mohamad Forouzanfar), they will potentially be maliciously accessed, creating risk to the provider and user of both systems. In order to avoid compromising individual citizen privacy while addressing the complexities created by the digital transformation of the nation of India, there needs to be dialogue on an interdisciplinary basis among those who create the laws, those who develop these technologies, and those who support or enforce civil liberties (Osama, Ateya, and Sayed et al. 2023). A balance that supports the advancement of AI, as well as protecting the rights of humans, is the best way for India to manage its digital transformation and protect the citizens' privacy.[27]

6. Balancing Individual Privacy Concerns with the Use of AI Surveillance Under India's Legal and Societal Framework

The implementation of AI-based surveillance technology in India has caused a serious legal crisis where there is a huge gap between the advancing technological capabilities and the current state of regulatory oversight. The state of India is using "intelligent infrastructure," such as large networks of sensors and predictive analytic technology, to improve the delivery of governmental services and therefore exposes considerable "regulatory gaps" in the laws that govern these activities (Mirakhori and others 2025). The current laws are increasingly ill-equipped to address the nuances of algorithmic decision-making, leaving citizens vulnerable to what scholars' term "sociotechnical harms." (Shelby, Shalaleh, and Kathryn et al. 2023). These harms are not merely theoretical; they manifest as tangible risks where the deployment of surveillance tools exacerbates existing social vulnerabilities, ranging from representational bias in data sets to the unauthorized commodification of personal information.[28] Consequently, the challenge facing Indian policymakers is not simply one of adoption, but of reconciliation: how to harness the security dividends of AI without dismantling the constitutional right to privacy (Reis, Nkechi, and Benedicta et al. 2024).

A primary point of friction is the opacity of these systems, often referred to as the "Blackbox Dilemma." (Rodriguez 2025). AI-enabled surveillance is run as an organization's secret and isn't open to public scrutiny due to the lack of sturdy transparency in regard to legislation (Das 2024). The lack of "transparent governance" creates a dilution of trust that exists between the government and the citizens regarding their public safety. Research has shown that absent of clear laws which enforced governance, these new technologies have the potential to work as a way of social sorting[29]; therefore, unfairly targeting lower-income, minority and marginalized communities while also digitalizing the systemic abuse they have suffered through generations.[30]

Furthermore, these new technologies also have a "balancing act" that is complicated by the fact that they can serve both beneficial and harmful purposes. Emerging technologies such as generative AI or Internet of Medical Things (IoMT) can cause many sectors (for example, education, healthcare) to undergo radical transformation by creating new opportunities, as well as significant privacy-related challenges (Varnosfaderani and Mohamad 2023). For example, while AI can dramatically help with improving the quality of clinical decisions, it will also require processing massive amounts of sensitive personally identifiable information (or PII), which raises ethical dilemmas related to consent and data sovereignty (Adel 2023). Because of these ethical dilemmas, many experts advocate moving toward "Industry 5.0" principles that place greater value on human-centered co-creation and ethical resilience rather than just operational efficiency (Aldoseri, Khalifa and Abdel 2024). In order to accomplish this, there must be an "elegant conversation" between technology experts, law academics, and civil liberties advocates, in order to develop a regulatory structure that is more anticipatory than reactively developed.[31]

Ultimately, achieving a sustainable equilibrium requires more than just patchwork regulation; it demands a fundamental restructuring of how surveillance is governed. Effective strategies must move beyond binary debates of security versus privacy to

---

24 Sheeja (n 2); see also Mirakhori (n 4).

25 *Ibid*.

26 *Ibid*.

27 Mirakhori (n 4); see also Reis (n 4).

28 *Ibid*.

29 Rodriguez (n 5); see also Shelby (n 2).

30 Rodriguez (n 5).

31 Mirakhori (n 1).

embrace a "harm reduction" taxonomy, ensuring that every deployment of AI is accompanied by rigorous privacy impact assessments.[32] Only by closing the current regulatory gaps and enforcing strict adherence to ethical standards can India ensure that its digital transformation serves as a tool for democratization rather than a mechanism for unchecked control.[33]

7. Strategies for Harmonizing National Security Interests with Privacy Rights through Policy, Technology, and Public Awareness Initiatives

Balancing the imperatives of national security (as driven by impending terrorism threats) with maintaining the rights of individuals to have their privacy respected will require implementing a strategy that transcends simplistic, binary trade-offs. Given that AI surveillance technologies are rapidly evolving, most recently illustrated by moving from reactive to predictive "intelligent oversight", the ability to establish and implement effective governance structures will continue to diminish. In order to successfully harmonize both of these imperatives, a tripartite approach will be needed to develop comprehensive policy frameworks, human-centric technological design, and proactive public awareness initiatives.

7.1 Policy Frameworks: Moving Beyond "Regulatory Gaps"

The first off-shoot of the policy is the closure of "regulatory gaps" which currently allow surveillance technology to grow faster than legal oversight. A more specific approach needs to exist, beyond global mandates, to have legally enforceable statutes that consider the nuances involved in "algorithmic governance". One example of this is the EU (European Union)'s A.I. Act, which does an astonishing job of implementing a "risk-based" approach to A.I. technology. For example, applications that are classified as "unacceptable-risk" (e.g., social scoring); will be outright banned, however, on (or are subject to) very strict requirements of transparency in the use of high-risk technologies (e.g., biometric identification) (Santoro and Anonymous 2025). This is in direct contrast to the "state-centric" model (for technology regulations) that is evident in China, where state/party stability and the state's interest in control of a national economy supersede the individual rights of individuals; thus, creating an environment where the Chinese government uses A.I. technology as a mechanism for "nation-building" or as part of their "techno-nationalistic" agenda.

The problem for countries, including India and the USA, is to create laws that ensure "black box" algorithm auditing processes don't inhibit creativity (Clayton 2024). In the US, legislative proposals such as the Eliminating Bias in Algorithmic Systems Act of 2024 (H.R. 10092) are designed to require that civil rights offices at all federal agencies actively combat algorithmic discrimination. A similar solution could be to create independent oversight bodies similar to the Digital Platform Commission (proposed), which will verify predictive policing tools aren't devolving into a new "Digital Jim Crow" and will help safeguard historically underrepresented and vulnerable groups of people from automated bias.

7.2 Technological Interventions: Industry 5.0 and Privacy-by-Design

The requirement for reconciling safety and privacy using technology requires an evolution to "Industry 5.0." This evolution prioritizes (1) multi-stakeholder, human-to-human collaboration, and (2) ethical resiliency over operational efficiency. The emergence of "Privacy-by-Design" supports the embedding of data safeguards into the architecture of surveillance systems at their respective architectures earliest phases.[34]

In addition, establishing solutions that mitigate "sociotechnical harm" requires organizations to address the Blackbox Dilemma by mandating the audit of all algorithms. Algorithmic audits will serve as a means by which the proprietary nature of the respective algorithms is not subject to public scrutiny, especially when the use of the respective algorithms impedes upon Fourth Amendment rights and international counterparts.

7.3 Public Awareness and Workforce Resilience

In defining a resilient security architecture, it also depends on having an informed citizenry and work force. Thus, public awareness programs focus on educating the public about the digital rights they have and the capabilities of surveillance technologies, thereby creating a culture of "transparent governance." This includes transparent disclosures about the use of "digital doppelgangers," or AI-generated duplicates of highly performing employees, for the purpose of ethically managing issues of compensation and consent.[35]

In addition, the "cyberattack surface" for cyber threats continues to grow due to the Internet of Things (IoT). Public education regarding good cyber hygiene is a critical national defense issue. By promoting an "inclusive policy approach" that includes technologists, civil rights activists, and the public, states can create an environment in which people can have confidence and trust in national security initiatives, rather than fear them.

8. Conclusion

The integration of artificial intelligence into the apparatus of national security represents a double-edged sword: it offers the unprecedented ability to "see, sense, and safeguard" populations while simultaneously threatening the very civil liberties it is designed to protect. As this research has elucidated, the transition from reactive monitoring to predictive "intelligent oversight" is no longer a futuristic concept but an operational reality. In India, the Smart Cities Mission represents a clear move towards the use of data-informed governance. The deployment of over 84,000 surveillance units demonstrates this shift towards using data to inform decisions about how to govern. However, the speed at which new technologies are being adopted outpaces the development of appropriate laws and regulations to address them; this has created a "regulatory gap," which creates a wide variety of "sociotechnical

---

32 Shelby (n 2).

33 Das (n 6); see also Reis (n 4).

34 *Privacy Tools Guide: Website for Encrypted Software & Apps* (v19.84, 2026).

35 McRae (n 12).

harms" to the public, ranging from the unauthorized commercializing of citizens' personal data to the subtle chilling impacts of being monitored continuously.

Importantly, the application of these technologies raises issues regarding the "Blackbox Dilemma". Increasingly more prevalent in law enforcement is the growing use of algorithmic decision making as evidenced through the increase in predictive policing systems. This creates a real risk of establishing "Digital Jim Crow". Without sufficient levels of transparency and auditability, these systems are likely to perpetuate historical biases, thus disproportionately impacting marginalized communities through the supply of objective mathematical certainties. The situation in India is more complicated than it is in both the European Union, which has developed a rights-based regulatory framework approach for balancing risk with fundamental rights and in China, where the government has opted for a top-down, state-based approach for achieving social control. Additionally, the decisions regarding how the governance of these technologies evolve will ultimately determine whether they become engines of democratization or instruments for "surveillance capitalism".

To reach Sustainable Development, we must shift from completely focusing on Technology-Based Solutions to creating people-oriented Solutions to bring People and Machines together through Resilient and Ethical Collaborations, instead of just looking at the most efficient way of doing things. Therefore, it is also important that we do not just have Strong Laws Around Algorithmic Accountability, but we also have an "Inclusive Approach" Creating Interdisciplinary Dialogue with Technology Professionals, Lawyers and Civil Society Groups. As the Generative Artificial Intelligence and the Internet of Things continue to create the "Attack Surface" of Critical Infrastructure, it is clear that you must not purchase National Security through the loss of Individual Privacy. Furthermore, there also needs to be "Nuanced Dialogue" for the Future so There are Strong and Powerful Security Infrastructures Duplicative of the Transparency Provided by them so that Security in the Digital Era can Enhance the Democratic Social Contract and not to be Used to Undermine this Contract.

References

Aaron Sankina and Surya Mattu. 2023. Predictive Policing Software Terrible At Predicting Crimes. *The Markup*. https://www.wired.com/story/plainfield-geolitica-crime-predictions/

Adel, Amr. 2023. Unlocking the Future: Fostering Human–Machine Collaboration and Driving Intelligent Automation through Industry 5.0 in Smart Cities. *Smart Cities* 6: 2742-2782. https://www.mdpi.com/2624-6511/6/5/124

Aldoseri, Abdulaziz, Khalifa N. Al-Khalifa and Abdel Magid Hamouda. 2024. AI-Powered Innovation in Digital Transformation: Key Pillars and Industry Impact. *Sustainability* 16: 1-25. https://www.mdpi.com/2071-1050/16/5/1790

B. Sheeja. 2025. Ethical Implications of Artificial Intelligence In Surveillance. *International Journal of Engineering Development and Research*: 763-766. https://rjwave.org/ijedr/papers/IJEDR2503076.pdf

Beraja, Martin, Andrew Kao, and David Yang, et al. 2023. Exporting the Surveillance State via Trade in AI. *Brooking*. https://www.brookings.edu/articles/exporting-the-surveillance-state-via-trade-in-ai/

Capraro, Valerio, Austin Lentsch, and Daron Acemoglu et al. 2024. The Impact of Generative Artificial Intelligence on Socioeconomic Inequalities and Policy Making. *PNAS Nexus* 3: 1-191. https://pubmed.ncbi.nlm.nih.gov/38864006/

Clayton Vickers. 2024. How AI Risks Creating a "Black Box" at the Heart of US Legal System. *The Hill*. https://thehill.com/business/personal-finance/4571982-ai-black-box-legal-system/

Das. Dilip Kumar. 2024. Exploring the Symbiotic Relationship between Digital Transformation, Infrastructure, Service Delivery, and Governance for Smart Sustainable Cities. *Smart Cities* 7: 806-835. https://www.mdpi.com/2624-6511/7/2/34

F Mirakhori and others, Balancing Individual Privacy Concerns with the Use of AI Surveillance under India's Legal and Societal Framework' (2025) 47.

Jagatheesaperumal, Senthil Kumar, Kashif Ahmad, and Ala-Al-Fuqaha et al. 2024. Advancing Education Through Extended Reality and Internet of Everything Enabled Metaverses: Applications, Challenges, and Open Issues. *IEEE Transactions on Learning Technologies.* https://ieeexplore.ieee.org/document/10415252/authors#authors

McRae, Emily Rose and Kaelyn Lowmaster. 2026. 9 Future of Work Trends for 2026. *Gartner*. https://www.gartner.com/en/articles/future-of-work-trends

Osama, Manar, Abdelhamied A. Ateya, Mohammed S. Sayed, and Mohamed Hammad et al. 2023. Internet of Medical Things and Healthcare 4.0: Trends, Requirements, Challenges, and Research Directions. *Sensors* 23: 1-36. https://www.mdpi.com/1424-8220/23/17/7435

Reis, Oluwatosin, Nkechi Emmanuella Eneh, and Benedicta Ehimuan et al. 2024. Privacy Law Challenges in the Digital Age: A Global Review of Legislation and Enforcement. *International Journal of Applied Research in Social Sciences*. https://www.semanticscholar.org/paper/PRIVACY-LAW-CHALLENGES-IN-THE-DIGITAL-AGE%3A-A-GLOBAL-Reis-Eneh/f539efb9f0d3a75fd95d4f0e6076 f3556a243d6b

Rodriguez, Fara Sheila. 2025. Predictive Policing: How AI is Setting the Stage for a Digital Jim Crow Era. *Congressional Hispanic Caucus Institute*: 1-4. https://chci.org/wp-content/uploads/2025/03/Rodriguez_ Fara_ Predictive-Policing-How-AI-is-Setting-the-Stage-for-a-Digital-Jim-Crow-Era-.pdf

Santoro, Michael A. and Anonymous. 2025. Deep Fakes and Surveillance Technology: Comparing the EU AI Act and Chinese AI Regulation. *Business Human Rights Journal.* https://bhrj.blog/2025/02/05/deep-fakes-and-surveillance-technology-comparing-the-eu-ai-act-and-chinese-ai-regulation/

Scoles, Sarah. 2019. Meet the US's Spy System of the Future — It's Sentient. *The Verge*. https://www.theverge.com/2019/7/31/20746926/sentient-national-reconnaissance-office-spy-satellites-artificial-intelligence-ai

Shelby, Renee, Shalaleh Rismani, and Kathryn Henne et al. 2023. Sociotechnical Harms of Algorithmic Systems: Scoping a Taxonomy for Harm Reduction. *Proceedings of the 2023 AAAI/ACM Conference on AI, Ethics, and Society* 723-741. https://dl.acm.org/doi/10.1145/3600211.3604673

Tariq, Usman, Irfan Ahmad, and Ali Kashif Bashir, et al. 2023. A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. *Sensors* 23: https://www.mdpi.com/1424-8220/23/8/4117

Varnosfaderani, Shiva Maleki and Mohamad Forouzanfar. 2024. The Role of AI in Hospitals and Clinics: Transforming Healthcare in the 21st Century. *Bioengineering* 11: 1-38. https://www.mdpi.com/2306-5354/11/4/337

Wadhawan, Vijay. 2025. Driving India's Intelligent Infrastructure with Next-Gen Solutions. *Primus Partners.* https://primus-partners.in/docs/documents/Infrastrcuture.pdf

Wikipedia. 2025. Artificial intelligence for video surveillance. https://en.wikipedia.org/wiki/Artificial_intelligence_for_video_surveillance accessed 17 October 2025

Wikipedia. 2025. Mass Surveillance in China. https://en.wikipedia.org/wiki/Mass_surveillance_in_China accessed 17 October 2025