UNIVERSITY OF WOLVERHAMPTON

BIRATNAGAR INTERNATIONAL COLLEGE

ing

BIRATNAGAR
INTERNATIONAL COLLEGE

Assignment II:

Term Paper on Ethical and Responsible AI

AI Surveillance, Facial Recognition & Civil Liberties: Ethical Challenges and Responsible Governance

Course: Concepts and Technologies of AI (5CS037)

Student Name: Kuldeep Mandal

Student ID: 2505925

Tutor: Ayush Regmi

Table of Contents

Abstract 3
1. Introduction 3
2. Thematic Review: AI Surveillance, Facial Recognition & Civil Liberties 4
2.1 Mass Surveillance and Human Rights Concerns 4
2.2 Facial Recognition and Peaceful Protest 4
2.3 Large-Scale Events and AI Surveillance: The 2024 Olympics 4
2.4 Bias, Accuracy, and Discrimination 5
2.5 Transparency, Consent, and Accountability 5
3. National and International Ethical AI Initiatives 5
4. Proposed Ethical AI Framework for Surveillance Systems 5
Fairness: 5
Transparency 6
Human Oversight 6
Accountability 6
Proportionality 6
5. Discussion 6
References 7

Abstract

The rise in the use of artificial intelligence (AI) surveillance systems and facial recognition has brought to the fore issues of privacy, freedom, and human rights. Though these tools are often employed in the name of safeguarding public safety and security, recent studies show how such tools can be used to affect mass surveillance, discrimination, and undue infringement of basic freedoms. This report presents an analysis of the ethical, constitutional, and social implications of AI surveillance systems, especially the use of facial recognition software in public gatherings, protests, and large-scale events, based on recent studies on academic papers and policy studies on the topic that have been published after 2021.

Key Words: AI Surveillance, Facial Recognition, Civil Liberties, Privacy, Human Rights

1. Introduction

Artificial intelligence has changed modern surveillance practices in a big way by making it possible to monitor things automatically, analyze data in real time, and identify people based on their biometrics on a scale never seen before. Facial recognition is one of the most controversial of these technologies because it can identify, track, and profile people in both public and private spaces. Governments are more and more using AI surveillance to deal with security threats, public disorder, and big events. However, recent studies suggest that these systems pose serious ethical, legal, and societal challenges.

One major concern is the erosion of privacy and security in public spaces. AI surveillance systems can continuously collect biometric and behavioral data, often without individuals explicit knowledge or consent. According to the U.S. Commission on Civil Rights, the absence of comprehensive legal frameworks governing facial recognition has allowed federal agencies to deploy these systems without consistent oversight or transparency, raising significant civil rights concerns. Additionally, AI surveillance systems are not immune to bias. Research demonstrates that facial recognition technologies can produce higher error rates for certain demographic groups, particularly racial minorities, women, and older individuals. Such inaccuracies can lead to wrongful identification, discriminatory enforcement, and violations of equal protection principles (U.S. Commission on Civil Rights, 2024)

Ethical AI frameworks emphasize fairness, accountability, transparency, and human oversight as essential characteristics of responsible systems. Recent international initiatives, such as the EU Artificial Intelligence Act, highlight the growing recognition that AI surveillance must be carefully regulated to protect fundamental rights. This report argues that without strong ethical safeguards and governance mechanisms, AI surveillance risks undermining democratic values and civil liberties despite its potential benefits for public safety.

2. Thematic Review: AI Surveillance, Facial Recognition & Civil Liberties

2.1 Mass Surveillance and Human Rights Concerns

AI-driven surveillance significantly enhances the capacity for mass monitoring. Facial recognition technologies can scan large crowds, match images against databases, and track individuals over time. The (U.S. Commission on Civil Rights, 2024) reports that federal agencies such as the Department of Justice and Department of Homeland Security use facial recognition across law enforcement and border control contexts, often without standardized accuracy testing or public reporting.

Mass surveillance raises concerns under fundamental human rights frameworks, particularly the right to privacy and freedom of expression. When individuals are aware they may be continuously monitored, they may alter their behavior, resulting in a chilling effect on democratic participation. This concern is especially pronounced in contexts such as protests and political gatherings.

2.2 Facial Recognition and Peaceful Protest

Academic research highlights the risks posed by facial recognition during peaceful protests. (Gabrielli, 2025) argues that the use of facial recognition in protest settings facilitates indirect mass surveillance by enabling the identification of participants, potentially deterring individuals from exercising their rights to assembly and expression. The study emphasizes that such practices may violate proportionality requirements under European human rights law, even when introduced under public order justifications.

Similarly, the UK Parliamentary briefing on live facial recognition notes that law enforcement use of these technologies in public spaces remains controversial due to limited transparency, unclear legal authority, and concerns over accuracy and bias, particularly in crowd-control situations.

2.3 Large-Scale Events and AI Surveillance: The 2024 Olympics

The deployment of AI surveillance during major events illustrates how temporary security measures can expand surveillance infrastructures. The Manchester Metropolitan University report on AI-driven mass surveillance at the 2024 Olympics explains that French authorities authorized AI-powered video surveillance to detect predefined “abnormal behaviors” such as crowd surges or abandoned objects. (Koula, 2024)

Although facial recognition was formally excluded, the report warns that continuous monitoring of millions of individuals still constitutes a significant intrusion into privacy. The authors highlight risks of false positives, biased categorization, and the normalization of emergency surveillance measures that may later become permanent.

2.4 Bias, Accuracy, and Discrimination

Evidence from the U.S. Commission on Civil Rights demonstrates that facial recognition systems often exhibit demographic disparities in accuracy, with higher false-positive rates for Black individuals, women, and older adults. Such disparities can lead to wrongful arrests, denial of services, or discriminatory treatment.

The report by (Bodim, 2025) published in IJFMR study further emphasizes that algorithmic bias and opaque decision-making processes undermine public trust and exacerbate social inequalities. The authors argue that without human-in-the-loop oversight, AI surveillance systems risk amplifying existing structural discrimination.

2.5 Transparency, Consent, and Accountability

A recurring ethical issue is the lack of meaningful consent and transparency. Individuals subjected to AI surveillance rarely have the ability to opt out or challenge automated decisions. (Transparency International, 2025)'s working paper warns that weak governance structures increase the risk of corruption, abuse of power, and misuse of AI surveillance data. Clear accountability mechanisms are therefore essential to prevent rights violations.

3. National and International Ethical AI Initiatives

Recent regulatory efforts reflect growing concern over the civil liberties implications of AI surveillance. The European Union Artificial Intelligence Act (2024) introduces a risk-based regulatory framework, classifying real-time biometric identification as a high-risk practice and prohibiting its use by law enforcement except in narrowly defined and exceptional circumstances, such as preventing serious crime or terrorism.

Similarly, the U.S. Commission on Civil Rights highlights the absence of comprehensive federal regulation governing facial recognition technology and recommends mandatory real-world accuracy testing, publicly accessible use policies, and statutory mechanisms for legal redress for individuals harmed by misuse or misidentification (U.S. Commission on Civil Rights, 2024).

4. Proposed Ethical AI Framework for Surveillance Systems

Fairness:

Fairness is one of the most important requirements for AI surveillance systems, especially facial recognition technologies. These systems rely heavily on training data, and if the data does not represent different genders, ethnicities, or age groups equally, the results can be biased. In practice, this means some people may be misidentified more often than others, leading to unfair treatment or discrimination. Regular bias testing and the use of diverse datasets help reduce these risks and ensure that AI systems treat individuals more equally rather than reinforcing existing social inequalities.

Transparency

Transparency means that people should know when and why AI surveillance systems are being used. Public authorities and organisations must clearly explain the purpose of surveillance, where it is deployed, and how collected data is stored and used. When surveillance operates in secrecy, individuals are unable to understand or challenge decisions that may affect their rights. Open communication and public disclosure increase trust and allow citizens to hold institutions accountable for how these technologies are used.

Human Oversight

AI systems should support human decision-making, not replace it. Human oversight ensures that automated outputs, such as facial recognition matches or alerts, are carefully reviewed by trained personnel before any action is taken. AI results can be inaccurate or misleading, especially in complex real-world situations. Keeping humans involved helps prevent blind reliance on technology and reduces the risk of serious harm, such as wrongful arrest or unnecessary surveillance.

Accountability

Accountability ensures that someone is responsible when AI surveillance causes harm. If an AI system is misused or produces harmful outcomes, there must be clear legal and institutional responsibility. Individuals affected by errors or misuse should have access to complaints mechanisms and legal remedies. Without accountability, mistakes can be dismissed as technical failures, leaving people without protection or justice.

Proportionality

Proportionality requires that AI surveillance is used only when it is genuinely necessary. Surveillance should be limited to specific situations, such as serious security threats, and should not involve constant or blanket monitoring of the public. Authorities should always consider less intrusive alternatives before deploying AI surveillance. This principle helps prevent the gradual expansion of surveillance into everyday life and protects fundamental freedoms such as privacy and freedom of expression.

5. Discussion

This research highlighted how AI surveillance technologies can profoundly affect civil liberties if deployed without ethical safeguards. While such systems promise efficiency and enhanced security, they also risk normalizing intrusive monitoring and weakening democratic freedoms. I learned that facial recognition is not merely a technical tool but a powerful mechanism that reshapes power relations between citizens and the state.

What stood out most was how easily temporary surveillance measures, such as those introduced for large-scale events can become permanent infrastructures. The documented biases and lack of transparency further reinforce the need for human oversight and accountability. Ethical AI is therefore essential not only for protecting individual rights but also for maintaining public trust.

Responsible AI development offers a pathway to balance innovation with human dignity. By embedding fairness, transparency, and legal safeguards into AI surveillance systems, societies can benefit from technological progress without sacrificing civil liberties. The long-term societal impact of AI will depend on whether ethical considerations are treated as core design principles rather than afterthoughts.

References

Bodim, M. (2025). *AI-Powered Surveillance vs. Privacy Rights: Striking the Right Balance.* International Journal for Multidisciplinary Research (IJFMR).

Gabrielli, G. (2025). The Use of Facial Recognition Technologies in the Context of Peaceful Protest: The Risk of Mass Surveillance Practices and the Implications for the Protection of Human Rights. *European Journal of Risk Regulation*.

Koula, D. (2024). *AI-Driven Mass Surveillance at the 2024 Olympics: Human Rights Issues and Recommendations.* Manchester Metropolitan University.

Oxley, G., Uwazuruike, A., Lalic, M., Samuel, H., & Downs, W. (2024). *Police use of live facial recognition.* UK Parliament.

Transparency International. (2025). *Addressing Corrupt Uses of Artificial Intelligence.* Transparency International.

U.S. Commission on Civil Rights. (2024). The Civil Rights Implications of the Federal Use of Facial Recognition Technology. *U.S. Commission on Civil Rights*.