

PAPER NAME

**AakashLopchan\_2548875\_AI\_report.doc  
x**

AUTHOR

**-**

WORD COUNT

**910 Words**

CHARACTER COUNT

**5610 Characters**

PAGE COUNT

**5 Pages**

FILE SIZE

**73.5KB**

SUBMISSION DATE

**Jan 16, 2026 11:41 AM GMT+5:45**

REPORT DATE

**Jan 16, 2026 11:41 AM GMT+5:45**

### ● 10% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

- 2% Internet database
- 3% Publications database
- Crossref database
- Crossref Posted Content database
- 10% Submitted Works database

3

Academic Year	Module	Assessment Number	Assessment Type
2026	5CS037/HJ1: Concepts and Technologies of AI (Herald College, Kathmandu, Nepal)	02	Report

*AI Surveillance, Facial Recognition & Civil Liberties*

*Student Name: Aakash Lopchan*

*Student ID: 2548875*

*Course: -5CS037*

*Submission Date: January 17, 2026*

## Table of Contents

Abstract .....	3
Introduction .....	3
Thematic Review.....	4
1 3.1 Mass Surveillance and Human Rights Concerns.....	4
1 3.2 Real-Time Facial Recognition in Public Spaces .....	4
3.3 Consent, Transparency, and Misuse .....	4
3.4 Balancing Safety with Civil Liberties .....	4
3.5 Proposed Ethical AI Framework for Surveillance .....	4
Discussion / Personal Reflection .....	5
References.....	5

# Abstract

AI has revolutionized surveillance through tools like facial recognition and vast data processing. These innovations boost security, reduce crime, and streamline administration, but they spark major ethical, legal, and societal issues. This report investigates the moral challenges of AI-driven monitoring, zeroing in on privacy, consent, civil rights, and responsibility. It delves into threats from widespread tracking and live facial ID in open areas, which can undermine core rights like free speech, personal independence, and fairness—particularly without proper checks or openness. The analysis covers dangers of abuse by authorities and businesses, such as biased targeting, unfair policing, and data expansion beyond initial goals. Drawing on global standards, it suggests a broad ethical model for AI monitoring to harmonize security needs with rights protection. Key takeaways stress the need for robust rules, oversight, and human involvement to keep AI surveillance beneficial without eroding democracy.

Key Words: AI Monitoring, Facial ID, Civil Rights, Privacy, Ethical AI

## Introduction

AI's role in surveillance has reshaped how communities detect, forecast, and tackle risks. Governments and companies now rely on facial ID, movement analysis, and forecasting models to improve safety, oversee cities, and curb offenses. Yet these advances bring deep worries about privacy, self-determination, equity, and rights. AI differs from old-school watching by offering nonstop, broad, automated oversight—often hidden from those affected, without their approval.

Ethical considerations in AI monitoring are vital since they touch basic human protections. Privacy, speech freedom, and gathering rights suffer under perpetual scrutiny, fostering self-censorship. Global standards like UNESCO's AI Ethics Recommendation, OECD guidelines, and the EU AI Act push for dignity, clarity, responsibility, and balanced use. True ethical AI demands equity, interpretability, rights respect, data security, and active human review.

To achieve this, creators and groups should build privacy into systems from the start, run evaluations, restrict data to essentials, and disclose operations openly. Solid rules, external checks, and liability measures are crucial too. This report spotlights AI monitoring

and facial ID as a key ethical flashpoint, probing the clash between safety-driven progress and rights safeguards in free societies.

## Thematic Review

### 3.1 Mass Surveillance and Human Rights Concerns

AI mass monitoring tracks huge groups via cameras, detectors, and data fusion nonstop. Promoted for security or crime-fighting, it triggers alarms over rights abuses. Round-the-clock watchfulness sparks caution, prompting people to change actions out of surveillance fear. This chills speech, grouping, and activism—bedrocks of open societies. Without firm legal limits, these tools can shift from safety aids to control mechanisms.

### 3.2 Real-Time Facial Recognition in Public Spaces

Facial ID tech spots and follows people instantly in places like roads, terminals, and gatherings. It helps find lost individuals or suspects, but wrong uses carry heavy ethical baggage. Studies show it errs more with women, minorities, and underserved groups, causing bias and false accusations. Unchecked rollout erodes public anonymity and habituates intrusive tracking.

### 3.3 Consent, Transparency, and Misuse

Lack of awareness and openness plagues AI monitoring ethics. People seldom know their data's capture, location, or application. Officials and firms often redirect footage from stated aims—a shift called scope drift. Absent controls, systems enable suppression, marketing exploitation, or biased policing. True ethics demands clear laws, open reporting, and simple breakdowns of practices.

### 3.4 Balancing Safety with Civil Liberties

Weighing security against rights is a core dilemma. Monitoring must stay targeted, essential, and measured—not blanket. Protections like court review, human veto power, and periodic checks preserve equilibrium. The EU AI Act labels live biometrics high-risk, mandating tight controls or prohibitions in some cases. UNESCO and OECD stress rights defense and answerability.

### 3.5 Proposed Ethical AI Framework for Surveillance

An adaptable ethical model for AI monitoring includes:

- Fairness: Block biased matching and unequal treatment.
- Transparency: Spell out goals, range, and constraints plainly.

- Human Oversight: Guarantee real human input in choices.
- Accountability: Pin down liability for errors or damage.
- Proportionality: Confine use to justified, legal ends.
- Sustainability: Weigh impacts trust and democracy over time.

## Discussion / Personal Reflection

Exploring AI monitoring and facial ID revealed technology's grip on personal liberty and cultural norms. Ethics count because unchecked systems can embed rights erosions under a neutral tech guise. The real issue lies in authority dynamics, oversight, and rules—not the tech alone. While offering safety and speed gains, absent protection, it deepens divides and shatters confidence.

Ethical integration from inception to rollout is key. Openness, approval, and human checks aren't extras—they're musts for trust. Following these can steer AI to equitable, secure results, sparing at-risk groups. Ultimately, principled surveillance bolsters democracy; reckless use breeds doubt, division, and rights decay. Societies' future hinges on navigating this tech-rights tightrope.

## Appendix

2

## References

UNESCO. (2021). *Recommendation on the Ethics of Artificial Intelligence*.

OECD. (2019). *OECD Principles on Artificial Intelligence*.

European Union. (2024). *EU Artificial Intelligence Act*.

5

NIST. (2023). *AI Risk Management Framework (AI RMF)*.

6

Lyon, D. (2018). *The Culture of Surveillance*. Polity Press.

4

Zuboff, S. (2019). *The Age of Surveillance Capitalism*. PublicAffairs.

## ● 10% Overall Similarity

Top sources found in the following databases:

- 2% Internet database
- 3% Publications database
- Crossref database
- Crossref Posted Content database
- 10% Submitted Works database

### TOP SOURCES

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	<b>University of Wolverhampton on 2026-01-14</b> Submitted works	3%
2	<b>University of Wolverhampton on 2026-01-15</b> Submitted works	2%
3	<b>University of Wolverhampton on 2025-02-11</b> Submitted works	2%
4	<b>American Intercontinental University Online on 2026-01-12</b> Submitted works	1%
5	<b>akinbobolaadedotunprincess.wordpress.com</b> Internet	<1%
6	<b>Changrong Lu. "Disciplining the Digital Public:Platform Mechanisms an...</b> Crossref posted content	<1%