AI Surveillance, Facial Recognition & Civil Liberties

Name: Biplov Maharjan

Student ID: 2462258

Tutor: Raju Karki

Module: Concepts and Technologies of AI

Abstract

Governments and businesses today are quickly turning to AI, like facial recognition, for everything from making money to keeping us safe and running things. These systems spark big ethical questions about privacy, rights, bias, and who's responsible, despite their potential for crime insight and making things run smoother. This piece considers available studies, policies, and human rights reports to judge the true ethical impact of AI monitoring. We've found big problems with how data is handled: tons of it are collected, things aren't clear, algorithms are biased, and there's not enough control. This study connects these technologies to dangers to democracy, using facts and global rules. Finally, we've got an ethical AI framework. It's meant to guide how we use surveillance tech responsibly, making sure fundamental rights are protected.

Introduction

Many surveillance systems now rely on artificial intelligence, and facial recognition is one of the most debated uses of it.Private companies use similar tools to protect systems and confirm identity, and many governments are expanding AI-based surveillance for public safety, border monitoring, and law enforcement. Despite these benefits, the rapid growth of AI-based surveillance has raised concerns about its effects on civil liberties, especially equality, privacy, and freedom of speech.

A key ethical issue with facial recognition is that it can support widespread, continuous monitoring in public spaces, often without people being clearly informed or having a real chance to agree or refuse. Reports from the OECD and the AI Now Institute warn that this type of surveillance can create a chilling effect. When people think they are being watched, they may be less likely to attend legal protests, speak openly, or take part in civic activities. Research in academic journals has found bias in facial recognition systems. In many evaluations, error rates are higher for women and for people with darker skin tones. When these tools are used in policing or by government agencies, these uneven error rates can contribute to unfair or discriminatory decisions, such as wrongful identification.

From an ethical standpoint, these issues align with key concerns in responsible AI, such as clear responsibility for outcomes, openness about how decisions are made, fair treatment across groups, and real human oversight that can guide or stop the system when needed. From a human rights perspective, AI should be used only when it is appropriate and needed, and its use should be governed by clear, transparent rules and procedures. To identify remaining gaps, this study surveys prior scholarship and policy initiatives and evaluates AI surveillance against these ethical principles.

Thematic Review

1. AI Surveillance and Civil Liberties

The studies I reviewed often point out that when AI surveillance is used without clear safeguards, it may threaten civil liberties. Policy reviews from the AI Now Institute and the OECD state that facial recognition can enable large-scale surveillance because it allows ongoing monitoring of people in public spaces. This undermines the basic democratic idea that people should be able to join public life without having their identity exposed. Research suggests that this kind of surveillance is used more often in disadvantaged communities than in others, which can widen existing power gaps between the public and the government.

2. Algorithmic Bias and Discrimination

Many academic studies, including work on algorithmic accountability, find that facial recognition systems can perform differently across demographic groups. This pattern often points to training data that does not represent the full range of people the system is supposed to identify, along with design decisions that were not carefully tested across different groups. These biases may lead to incorrect identification, especially in law enforcement contexts. Because these mistakes put justice and equal treatment under the law at risk, they are not just technical problems; they are ethical violations. Studies indicate that monitoring technologies that contain bias can introduce discrimination into routine institutional work and allow it to spread across different settings.

3. Transparency and Explainability

Several studies note that AI-based surveillance systems can be hard to evaluate because they do not clearly explain the steps behind their decisions. Many facial recognition systems operate as black boxes, which means people affected by their decisions cannot see what factors led to a match or error, and they have little basis to question or appeal the result when the system is wrong.Policy guidelines note that transparency is needed to keep public trust and to support accountability. Oversight procedures often fail when they are not clearly explained, since reviewers may miss misconduct and allow it to pass through the review process.

4. Accountability and Governance Gaps

Several studies point to a clear gap in accountability in how AI surveillance is used. It is often hard to determine who should be held responsible for harm caused by AI systems, whether that is the developers, the sellers, or government agencies. When responsibility is spread across many people or units, it becomes harder to identify who is accountable, which can weaken both legal and ethical responsibility. To address this gap, international efforts such as the Toronto Declaration and policy studies in Europe call for required impact assessments, clear and transparent governance rules, and independent audits.

5. Existing Initiatives and Regulatory Responses

To address these risks, governments and institutions are introducing policy measures.EU proposals and OECD principles call for proportionate rules, real human oversight, and governance based on fundamental rights.Civil society groups say real-time facial recognition in public should be paused or banned until clear rules, independent oversight, and strong privacy and rights safeguards are in place. Ethical risks are getting more attention, but uptake and enforcement still differ widely by country.

6. Proposed Generic Ethical AI Framework

When thinking about ethical AI for surveillance systems, it's important to consider more than just technology. A responsible approach should include:

- Fairness: Make sure the AI treats everyone equally by regularly checking for biases, using diverse datasets, and preventing discriminatory outcomes.
- Transparency: Be open about what the system does, where the data comes from, and how decisions are made.
- Human Oversight: Keep humans in the loop, especially for high-stakes decisions like law enforcement actions.
- Accountability: Clearly define who is responsible at every stage of the AI system's life, and ensure there are ways for people to challenge or correct mistakes.
- Sustainability: Deploy AI in ways that respect democratic values and maintain public trust.

By combining technical safeguards, ethical principles, and clear governance, this framework helps guide the responsible use of AI in surveillance.

Discussion / Personal Reflection

Studies of AI surveillance and facial recognition suggest that rapid technical progress can conflict with basic human rights when ethical limits are not taken seriously.Research in this area argues that AI is not neutral, since it can reflect existing social biases, unequal power relations, and the policy choices made during its design and use.If AI-based surveillance is used without clear ethical safeguards, it can make large-scale monitoring feel routine and can erode civil liberties, even when it is justified in the name of efficiency or public safety. Ethical considerations should be part of AI design, testing, and deployment from the outset, rather than being added after the system is already in use. Fairness, transparency, and accountability are basic practical standards that help reduce the risk of harm in everyday settings.This ethical AI framework argues that innovation in AI should move forward in line with human rights principles. This topic argues that computer scientists and policymakers should ask not only what AI is able to do, but also what it should do. As automated systems become more common, ethical AI is needed to protect public trust, democratic processes, and individual freedom.

Reference

AI Now Institute. (2019). AI Now report 2019: The social and economic implications of artificial intelligence technologies.
https://ainowinstitute.org/wp-content/uploads/2023/04/AI_Now_2019_Report.pdf

American Civil Liberties Union. (2019). The dawn of robot surveillance: AI, video analytics, and privacy.
https://www.aclu.org/publications/dawn-robot-surveillance

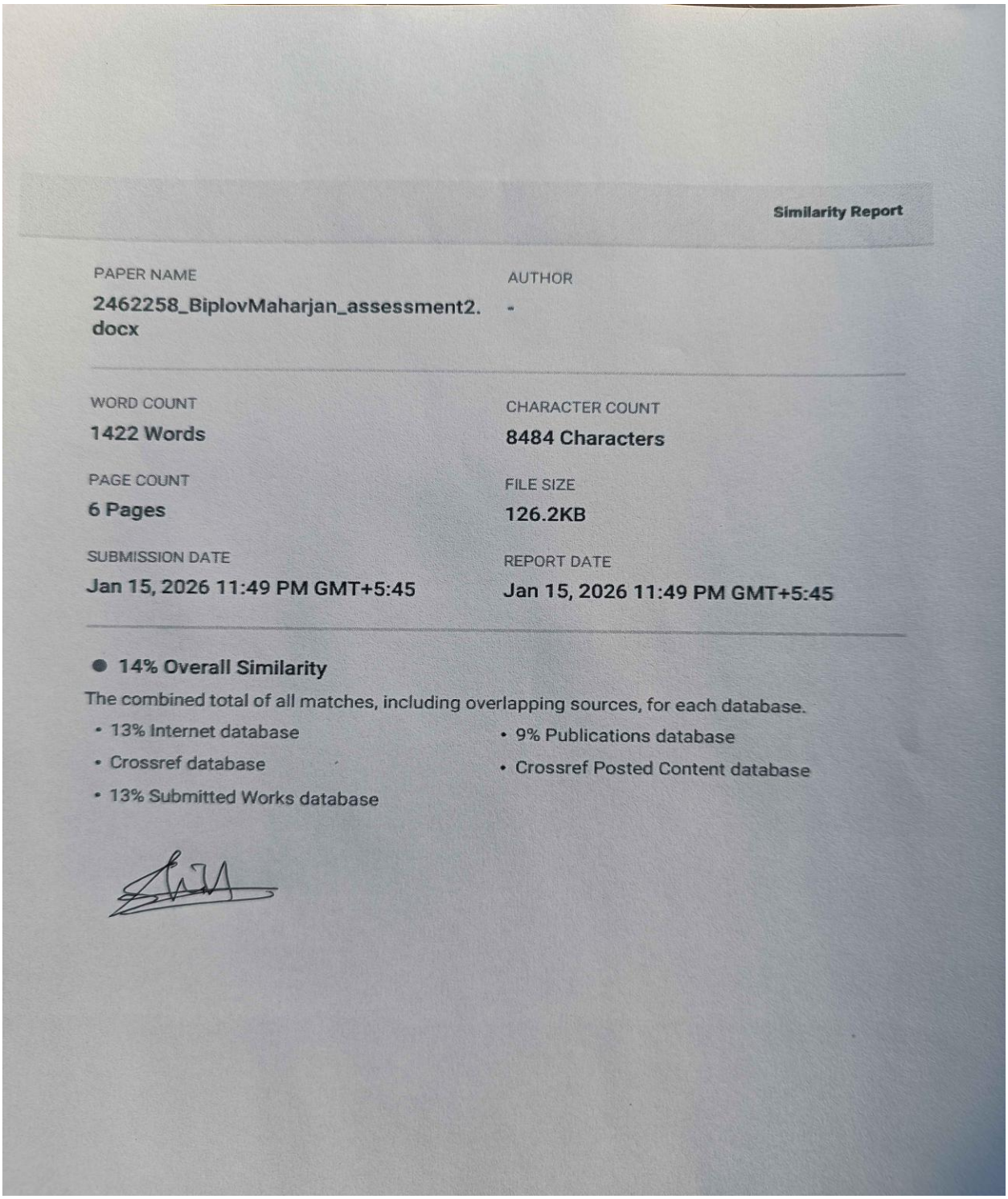
European Parliament. (2024). Artificial intelligence and human rights: Using AI as a weapon of repression.
https://www.europarl.europa.eu/RegData/etudes/IDAN/2024/754450/EXPO_IDA(2024)754450_EN.pdf

Organization for Economic Co-operation and Development. (2019). Artificial intelligence in society. OECD Publishing.
https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/06/artificial-intelligence-in-society_c0054fa1/eedfee77-en.pdf

Raji, I. D., Smart, A., White, R. N., Mitchell, M., Gebru, T., Hutchinson, B., Smith-Loud, J., Theron, D., & Barnes, P. (2020). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing.
Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (FAccT).
https://arxiv.org/abs/2001.00973

Wachter, S., Mittelstadt, B., & Russell, C. (2020). Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI.
Computer Law & Security Review, 41.
https://arxiv.org/abs/2005.05906

Appendix



Similarity Report

PAPER NAME
2462258_BiplovMaharjan_assessment2.docx

AUTHOR
-

WORD COUNT
1422 Words

CHARACTER COUNT
8484 Characters

PAGE COUNT
6 Pages

FILE SIZE
126.2KB

SUBMISSION DATE
Jan 15, 2026 11:49 PM GMT+5:45

REPORT DATE
Jan 15, 2026 11:49 PM GMT+5:45

● 14% Overall Similarity

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

- 13% Internet database
- 9% Publications database
- Crossref database
- Crossref Posted Content database
- 13% Submitted Works database