Essay

“Ethical Concerns and Security Risks of Facial Recognition Technology”

Aftab Alam Masjidi

CS-318: Biometric Methodologies

Barry University

Professor Bass

April 22, 2025

“Ethical Concerns and Security Risks of Facial Recognition Technology”

Facial recognition technology (FRT) is rapidly growing biometric technology that verifies or identifies individuals on the basis of their facial structure. It is increasingly being employed in airports, shopping malls, police stations, and mobile phones. Even though the technology is providing convenience and security, it also poses very serious moral issues and security risks. The most significant moral issues connected to facial recognition are invasion of privacy, lack of provision of informed consent, bias in algorithm, and data breach potential.

One of the most contentious ethical concerns with FRT is the invasion of privacy. The technology can identify people without their consent or awareness, particularly in public places. Facial recognition cameras can track people around and observe their activities all the time. It raises questions about whether individuals are ever truly anonymous when they are in public places. As Toxigon (2024) describes, such broad-based monitoring has a "chilling effect" where people feel discouraged from speaking their minds, especially in sensitive contexts such as political protests or religious services. The issue of ethics is not just gathering the data but transparency as to who is gathering it and why.

Lack of notification to subjects is closely linked to issues of privacy. The majority of subjects are not aware at and where precisely their facial information are being collected and stored. Unlike the majority of other biometric technologies like fingerprint analysis, FRT permits remote deployment with no physical interaction. The benefit here rests with businesses or state agencies where such applications could continue unending without end users' consent. In a democratic state, protecting autonomy at the level of the individual and upholding the doctrine of consent when it comes to the harvesting of personal information is important. According to the U.S. Government Accountability Office (GAO, 2020), commercial facial recognition has largely occurred in the retail or advertising context in ways that did not inform consumers nor their ability to opt out, reducing ethical standards of transparency and respect for personal space.

Algorithmic bias is also a major concern. Research has shown that facial recognition algorithms are less accurate when dealing with women and darker-skinned individuals. These inaccuracies lead to adverse consequences, especially in law enforcement, where FRT is used for suspect identification. A study cited by the Financial Times (2024) indicated that deployment of face recognition by the UK Metropolitan Police resulted in false positives within the people of color community. This is a concern in terms of racial discrimination, as discriminatory algorithms can cause wrongful arrest or targeting of certain communities. The problem is typically that the data upon which these systems are trained might not have representative diversity within all groups of populations. Without modifying these biases, FRT will continue to perpetuate the current social inequalities.

In addition to the ethics concerns, facial recognition systems are also vulnerable to security breaches. As compared to passwords or identification codes, facial features or biometric data like facial patterns are irrevocable once compromised. Once a hacker gains entry into a facial data database, the victim cannot easily replace his or her "face" as one does when resetting a password. According to the GAO (2020), weak cybersecurity measures in commercial and government FRT systems have left them susceptible to malicious attacks. The risk of identity theft, fraud, and misuse of personal data is high if such confidential information is not suitably protected.

In conclusion, while facial recognition technology has practical benefits, it poses serious ethical concerns and security risks. The ability to track people without consent, combined with biased algorithms and weak data protection, undermines human rights and social justice. In order to avoid misuse, developers and policymakers must have clear guidelines that prioritize transparency, consent, and security. By addressing these issues, society can reap the rewards of FRT without undermining ethics.

References

Financial Times. (2024). Met police use of facial recognition in London surges. https://www.ft.com/content/c33322a7-eba7-4299-8172-4ce1d4e88908

Toxigon. (2024). Ethics in facial recognition technologies: A comprehensive guide. https://toxigon.com/ethics-in-facial-recognition-technologies

U.S. Government Accountability Office. (2020). Facial recognition technology: Privacy and accuracy issues related to commercial uses (GAO-20-522). https://www.gao.gov/products/gao-20-522