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

Essay

“The Integration of Artificial Intelligence in Biometric Systems”

Aftab Alam Masjidi

CS-318: Biometric Methodologies

Barry University

Professor Bass

April 24, 2025

“The Integration of Artificial Intelligence in Biometric Systems”

Artificial Intelligence (AI) has fundamentally transformed various sectors, biometrics being one of them. Biometrics is a term that is used to define technology utilized to recognize and verify an individual on the basis of remarkable physical or behavioral traits. AI deployment in biometric systems has enhanced their speed, precision, and responsiveness, setting a new standard for security and identity verification.

The most significant of AI use in biometrics involves facial recognition. Deep learning technology is now capable of making systems recognize and identify faces at varying levels of light, angles, and even partial obstructions. It helps eliminate false positives and improve identification processes. AI has also improved fingerprint identification by deciphering poor or smudged prints. The previous systems would fail when reading such prints, but AI-driven models can learn and derive meaningful patterns to authenticate users better.

Iris recognition, already extremely accurate, has been reinforced further by AI. Perhaps the most stunning application is in identifying whether an iris is from a living or deceased individual to avoid spoofing using artificial or post-mortem samples. AI systems have performed remarkably well in this area, showcasing how deep learning can strengthen security even in edge conditions.

With the improvement of AI in biometric systems comes the new threats as well. For instance, today there are attackers who employ images and fingerprints produced by AI and referred to as "DeepMasterPrints" to trick recognition systems. Synthetic prints are designed to be compatible with multiple fingerprint templates, so they are indeed a threat to security. Also, data poisoning—altération of the input data used to train AI models—can corrupt system integrity and leave them vulnerable to future attacks (Yurdasen, 2023).

The use of AI-based biometric systems is growing in several sectors. At airports, facial recognition systems streamline security checks and boarding procedures by instantaneously matching faces of passengers with their passport photographs. At banks, AI-based voice and fingerprint recognition allow customers to safely log in without traditional passwords. Police use AI to recognize suspects in real time from public surveillance video, speeding up and refining investigations. Even cell phones now rely on AI-boosted facial and fingerprint readers to unlock devices, verify identities for transactions, and allow secure app access. Such everyday applications prove growing trust in AI-powered biometrics as a security and convenience solution (Yurdasen, 2023).

The increasing use of AI-based biometric data collection raises ethical and privacy concerns. Centralized storage of sensitive data renders systems an attractive target for cyberattackers. Furthermore, AI-based surveillance and emotion detection technologies raise essential questions about consent, control, and abuse. Some projects involving certain biometric AI have even been put on hold by some firms due to such ethical concerns, indicating the necessity of proper deployment and regulation.

AI has driven biometric systems to new heights by making them quicker, more accurate, and more responsive. From facial identification and fingerprint scanning to iris scan and behavioral monitoring, AI equips systems to authenticate individuals with greater confidence. But the benefits must be counterbalanced with careful consideration of potential threats and ethical implications. There has to be ongoing research, security innovation, and regulation to ensure that these powerful weapons are being used responsibly and securely in our increasing digital era (Yurdasen, 2023).

References

Yurdasen, D. (2023, April 20). *How artificial intelligence (AI) is used in Biometrics*. ARATEK.

https://www.aratek.co/news/how-artificial-intelligence-ai-is-used-in-biometrics

Essay

“Informed Consent and Biometric Identification”

Aftab Alam Masjidi

CS-318: Biometric Methodologies

Barry University

Professor Bass

March 27, 2025

"Informed Consent and Biometric Identification"

Introduction

Biometric identification has become the cornerstone of modern security and authentication systems, using unique physiological or behavioral characteristics such as fingerprints, facial recognition, iris scanning, and voiceprint patterns. These technologies are more secure and convenient but do pose genuine ethical concerns, most prominently informed consent. The traditional definition of informed consent requires users in aggregate to understand and voluntarily agree to the collection and storage of their personal data. However, biometric identification complicates this principle due to clandestine data collection, transparency, and evolving regulatory systems (Alterman, 2003). The present paper scrutinizes the challenge posed by biometric identification to informed consent and sets out the potential solutions that ensure ethical quality in biometric governance.

Background on Biometric Identification

Biometric systems recognize or authenticate persons by comparing stored biometric templates with live data. Common modalities include fingerprinting, face recognition, iris scan, and behavioral biometrics such as keystroke dynamics and gait recognition. In contrast to passwords or IDs, biometric identifiers are intrinsic to individuals, making them more difficult to forge or lose (North-Samardzic, 2020). However, that uniqueness also jeopardizes privacy insofar as, in contrast to the password, biometric data, once compromised, cannot be changed. As biometric technologies are increasingly applied within both public and private spheres, from airport checkpoints to mobile phone authentication, informed consent principles must be taken under serious consideration (Sprokkereef & de Hert, 2007).

Challenges to Informed Consent

Lack of Transparency

One of the critical issues of biometric identification is the transparent procedure of how information is collected, stored, and used. Many sign up to be scanned for their

biometric data without fully appreciating the implication. For example, face recognition software employed in public spaces may not always seek permission from the user, raising issues of unwitting participation (Alterman, 2003). Besides, governments and corporations also tend not to make data retention policy information clear and comprehensible, hence having an uninformed process of consent and not a voluntary one.

Covert Data Collection

Compared to the active involvement necessitated by traditional identification approaches, others capture information passively and unknowingly by users. Public places facial recognition cameras, behavior biometrics on online platforms, and voice identification on smart speakers all contribute to this issue. North-Samardzic (2020) cites the way that second-generation biometrics, which scan the user's behavior rather than fixed identifiers, render consent more complicated since the users do not even notice their biometric data is being processed.

Regulatory Gaps

Legal structures for the gathering of biometric information differ widely across jurisdictions, and are typically lagging behind technological advancement. While the European Union's General Data Protection Regulation (GDPR) makes provision for the protection of biometric data, its implementation is uneven (Sprokkereef & de Hert, 2007). There are no clear guidelines for seeking biometric consent in most regions, and this puts individuals at risk of abuse of their data. Absence of consistent world-wide rules increases the challenge of getting informed consent in biometric identification systems.

Function Creep

Function creep occurs when biometric information initially gathered for a specific purpose finds subsequent use for an additional purpose without additional consent. For instance, a firm collecting fingerprints for worker entry control can later utilize the same information for monitoring attendance and productivity without

employees' consultation (Cooper & Yon, 2019). The expanding use of biometrics beyond its initial purpose adds to erosion of the integrity of the consent process and provokes ethical concerns about data ownership and control.

Addressing the Ethical Concerns

In order to counter these challenges, certain steps can be taken to bolster informed consent in biometric identification.

1. **Enhanced Transparency**: Companies need to give explicit, detailed, and understandable explanations of biometric data collection, storage, and usage policies. This includes informing users of the possible risks and retention periods.
2. **Regulatory Strengthening**: Governments should enact and implement wide-ranging legislation that requires informed consent procedures at the time of biometric data collection. Such policies like those on medical data, requiring express and documented consent, could be taken as templates (Sutrop, 2010).
3. **User Control and Opt-Out Mechanisms**: Users ought to be permitted to view, modify, or delete their biometric data on demand in order to gain control over personal information.

The Role of Corporate Responsibility

Firms adopting biometric identification systems have an ethical obligation to provide informed consent and data privacy. Ethical business practice includes structuring consent policies to surpass legal requirements, giving users control over their biometric data. Transparency reports of the use of biometric data, third-party access policies, and encryption methods should be disclosed to the public to foster trust (North-Samardzic, 2020). Firms that do not put these ethical issues as a priority risk damaging their reputation and being legally prosecuted.

Public Perception and Trust in Biometric Systems

Support for biometric identification is based on institutional and technological trust as well as the handling of the biometric information. The high-profile status of reported breaches and suspect data practices contributes to suspicion. Increasing public knowledge about the value and risk of biometric technologies and giving them simple, transparent channels for data control can improve trust (Cooper & Yon, 2019). Governments and institutions must work together to put in place accountability structures that guarantee user rights and security are at the forefront.

Future Directions in Biometric Consent

With developing biometrics technology, the future of informed consent is also changing. De-centralized identity management and blockchain-based biometric storage are the new trends that offer promising paths for user autonomy and protection. Additionally, novel technologies in privacy-protecting biometrics, including homomorphic encryption and federated learning, potentially enable more secure authentication without exposing raw biometric data. Research into ethical applications of AI in biometrics must also be conducted to ensure that automated decision-making systems are open and responsible. By embracing such technologies, biometric systems will be able to balance the security needs with ethical responsibility to ensure a future where informed consent remains a corner stone of biometric identification.

Conclusion

Biometric identification seriously imperils the doctrine of informed consent, primarily due to absence of transparency, clandestine collection of data, regulatory loopholes, and creep of function. As biometric technologies are growing more advanced and penetrating more areas of everyday life, there is a need to put in place more effective ethical and legal safeguards. Stepping up transparency, enforcing clear consent mechanisms, strengthened regulatory oversight, and providing individuals with more control over their biometric information are key steps toward resolving such concerns. Otherwise, the very right of informed consent would be lost in the era of biometric identification.

References

Alterman, A. (2003). ``A piece of yourself'': Ethical issues in biometric identification. *Ethics and information technology*, *5*(3), 139-150.

Cooper, I., & Yon, J. (2019). Ethical issues in biometrics. *Science Insights*, *30*(2), 63-69.

North-Samardzic, A. (2020). Biometric technology and ethics: Beyond security applications. *Journal of Business Ethics*, *167*(3), 433-450.

Sprokkereef, A., & De Hert, P. A. U. L. (2007). Ethical practice in the use of biometric identifiers within the EU. *Law Science and Policy*, *3*(2), 177.

Sutrop, M. (2010, January). Ethical issues in governing biometric technologies. In *International Conference on Ethics and Policy of Biometrics* (pp. 102-114). Berlin, Heidelberg: Springer Berlin Heidelberg.