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.