BIOMETRIC DATA AS INTELLECTUAL PROPERTY: REDEFINING OWNERSHIP IN THE DIGITAL AGE

Parineeta Goswami[*]

Abstract

Biometric systems have brought changes in the operation of identification and authentication with enhanced efficiency and security in different operations or services. However, such methods raise set of ethical, legal, and social implications pertaining it. Nevertheless, biometric technologies raise algorithmic bias risks, the right to anonymity, public trust, and their relationship with intellectual property rights, on which this article is premised. Other biases identifiable with biomarkers evident in algorithms including face recognition algorithms are capable of worsening societal vices that farm injustice by discriminating against minority groups. However, surveillance in public spheres erodes liberties, serves as the sign of the emergence of surveillance in democracy, and limits speech freedoms for people. This is why biometric data is viewed with a lot of suspicion by users, and policies developed by international organizations seek to set high levels of transparency and maximum measures for protection from misuse or any other wrong intentions. This article also considers the prospects of protection of biometric data from the perspective of the intellectual property legislations, as well as the conflict between the rights of the person and the corporate ownership. Albeit, certain legal rights are made for the creation of new biometric technologies, these rights also tend towards the monopoly of systems and create new ethical questions related to data ownership and abuse. Solving these challenges requires overall regulatory systems that take into consideration the possibilities of new technologies at the same time as the rights of persons. Governments, engineers, and philosophers must join their efforts to make algorithms fair, answerable to the public and explainable. When issues of ethical aspects are incorporated into the algorithm and in the common and everyday installation of the biometric systems, then the intended benefits that come with this technology can be achieved without infringement on the rights of individuals. The author of this article therefore strongly supports egalitarian policies and standards with a view to fighting discrimination in the application of biometric technologies in a manner that upholds a given society's ethics.

[*] Assistant Professor, School of Law, UPES Dehradun.

Keywords: Biometrics, Algorithm, Transparency, Technology, Identification.

1. Introduction

Biometric identification systems have dynamically developed over the last hundred years moving from the most primitive methods of identification to the modern computerized identification methods that are used widely today for security measures, social identity, and surveillance systems. Biometrics can be said to have its roots in cases of early attempts at the identification of persons; the development and progress of biometrics have been shaped by several factors including bearing in mind technological innovation and development, the development of data processing systems, and indeed the social demands. A brief evolution of the technologies, including their development from the past to the present forms, like Face Recognition, Iris Scanning, and even Voice Identification are discussed in this section as well. Biometric identification traces its early use back to the beginning of ancient civilization. The Babylonians and the Chinese held the original formal knowledge about identity based on the physical characteristics of the people, including fingerprints. However, the systematic and scientifically validated use of biometrics originated at the end of the 19th century with the use of fingerprints.[1]

In 1892, a British Scientist named Sir Francis Galton made a detailed study of fingerprints and thus brought about conclusive proof as to their individuality and therefore as a means of identification. Sir Edward Henry came next with the database fingerprint classification system which is currently used by most of the police today. In the early part of this century, fingerprinting was incorporated into the crime-fighting tool kit to aid in the identification of criminals thus minimizing mishaps related to such aspects as mistaken identity. Nineteen centuries later, a fingerprint was widely used in the police headquarters of European and American nations.[2] Fingerprinting was not the only form of biometric identification that was researched, physiognomy or facial recognition was also considered. Although this method saw some form of popularity in the 19th and early

[1] Alan Gelb and Julia Clark, "Identification for Development: The Biometrics Revolution" (*Centre for Golbal Development Working Paper No. 315* (January 28, 2013), a*vailable at:* http://dx.doi.org/10.2139/ssrn.2226594 (last visited on March 07, 2025).

[2] Manpreet Singh Dhillon, "Pre-History of DNA Fingerprinting in India", 10(3) *Journal of Humanities and Social Sciences* 882-886 (2019).

20th centuries, it was brought down by the far more scientifically backed method of fingerprinting as the best form of identification.[3]

Over time, the twentieth century alone saw a need for a more sophisticated set of techniques for biometric identification because populations became larger, movements across borders intensified and criminals' work became more diverse and technical. This eventually brought improvement in the field of biometrics. The thought of using body characteristics such as the eye for identification was developed in the 1930s and 1940s. The first experimentations in iris recognition took place during this phase. Dr. Frank Burch and Dr. John D. Maynard at the University of Michigan carried out research that showed that the iris is different in every person and can be used as an identification tool. Though it was only in the last years of the 20th century that the technology became viable through the success of iris recognition, it originated the process.[4]

Voice recognition was in the early 1950s and 1960s discussed as another option for biometric identification. The initial voice recognition systems entailed the analysis of the voice's particular attributes, for instance, the tone, and pitch, or recommending a minimum of three reliable but unconventional voice recognition resources. However, two main sources of weakness were identified: Reduced accuracy and dependency on changes in voice resulting from health conditions, noise, or ageing. However, it still served a purpose in small degrees specifically for telephones for verifying an individual's identity. Biometric technology began evolving in the middle of the Second World War and was popularized in the last quarter of the twentieth century driven by the advances in digital computing that make data management much easier. During this period automated biometric systems were being developed which could automatically recognize people without interference from persons. The main technologies to emerge currently involve facial recognition, iris scanners, touch and fingerprint recognition.

Fingerprinting has been around for over a century and the introduction of automated fingerprint identification systems (AFIS) changed it. AFIS enabled fingerprints to be acquired as digital images, measured concerning their specific features and then searched against numerous databases within a shorter period than would have

[3] Paul Roberts, "Biometric Technologies: History and Applications" *Encyclopedia of Information Science and Technology* 524, 527 (Mehdi Khosrow-Pour ed., 3d ed. 2015).

[4] Simon Cole, *Suspect Identities: A History of Fingerprinting and Criminal Identification* 45 (Harvard University Press, 2009).

been achieved using manual methods. By the 1980s, AFIS had spread around the world for use by law enforcement which in turn resulted in faster identification of culprits and the preservation of many fingerprints.[5]

It was in the 1990s when the field of facial recognition had its first breakthroughs. This technology employs software to scan and analyze the exact locations of specific facial features such as the distance between two eyes, and the space between the nose and the mouth as well as turning this data into coordinates. Unlike fingerprinting and iris scanning, facial recognition is a non-intrusive biometric technology that can be carried from a distance, hence is very relevant in surveillance and security. The 1990s also featured the emergence of technologies which could map photographs with face databases, and such systems are now in use in airports, banks, and other buildings.[6]

Iris recognition is one of the biometric systems, which was a theoretical possibility from the early 1940s but became realistic only in the 1990s with the appearance of digital cameras for high magnification of the eye. The first algorithms were developed back in 1994 by Dr. John Daugman and they became able to identify persons using iris patterns. Iris recognition was integrated into security systems in the early 2000s that featured high-security areas including government offices, research facilities, and a few airports. Iris has stable and permanent features that developers find efficient to use over a long period and thus it is among the most efficient biometric identifiers.

As can be noticed, the use of biometric technologies across the 21st century has become as common in security as well as in popular usage. New technologies such as mobile phones, online shopping and calls for better, faster security systems have presented biometric technologies into people's everyday lives. In the early 2000s, the use of fingerprint sensors in smartphone devices can be considered a significant stage for biometric technology development. The start of biometric authentication for the consumer market began in 2004 when Apple launched its first mainstream smartphone, the iPhone 5s, with a fingerprint scanner. This was succeeded by the embodiment of fingerprint scanners with tablets, laptops and many other consumer products. Today,

---

[5] Michael Lynch, Simon A. Cole, *et. al.*, *Truth Machine: The Contentious History of DNA Fingerprinting* 78 (Chicago University Press, 2008).

[6] John Thornton, "The General Acceptance of Fingerprint Evidence in the United States" 26 *Journal of the Forensic Sciences Society* 492, 497 (1986).

fingerprint recognition is one of the most popular technologies applied to unlock gadgets, pay with, and protect internet accounts.[7]

Biometrics in particular, facial recognition technology has been growing at a very rapid pace over the years because of the need for security and surveillance. Starting from biometric unlocking of smartphones, up to video surveillance of cities, this technology has been used actively. In 2016, Apple unveiled the iPhone X, and the world was introduced to Face ID; the use of facial recognition for security and payment. Nevertheless, the application of an increasing attention to facial recognition has raised issues in privacy, reliability, and racial disparity in artificial intelligence decision-making.[8]

In parallel with these developments, voice recognition and behavioural biometrics have also progressed. Voice biometrics has been implemented in solutions such as smart speakers, e.g., Alexa, Siri; in banking where voice identification is applied to confirm customers by phone call. Furthermore, new more refined techniques including behavioural biometrics; work based on the pattern a particular user creates in his/her behaviour such as typing, mouse movement and even touch on the mobile device.[9]

Nevertheless, the quiet growth of biometric technologies and application proliferation continues to elicit substantial, intricate, and essential ethical, legal, and social questions. The general privacy concerns end up being dominant features of the biometric technology debate especially concerning storage, consent and potential exploitation of the data. Furthermore, there is always a risk of bias in algorithms, and this has been a major issue, especially in facial recognition techniques where a solution to the problem has yet to be developed. The advancement in Biometric technologies will remain vibrant in future. Solutions such as DNA biometrics, which are still under development, may introduce even wider applications of biometric identification. Further, any breakthroughs in artificial intelligence or machine learning could enhance current

[7] Mark S. Nixon and Alberto S. Aguado, *Feature Extraction & Image Processing for Computer Vision* 321 (Academic Press, 3rd ed., 2013).

[8] Andreas Holzinger, *et. al.*, "Trends in Interactive Knowledge Discovery for Personalized Medicine: Cognitive Science Meets Machine Learning" 275 *Procedia Computer Science* 17, 21 (2017).

[9] John Daugman, "How Iris Recognition Works" 14(1) *IEEE Transactions on Circuits and Systems for Video Technology* 21, 23 (2004).

biometric structures and designs, and simultaneously, create new methodology of identification that could minimize invasiveness.

2. Global Regulatory Landscape of Biometric Technologies

When creating the standards to govern the application of biometric technologies, regulators from different countries have been forced to address the subject to weigh the benefits of these technologies against the civil liberties of a nation's citizens. Fingerprints, face and voice identification and scans, iris scans, etc. are physically distinctive from one individual to another and very sensitive, and their collection, storage, and use also present a major privacy issue. To resolve these problems, different countries have adopted current national legislation or are gradually developing data protection laws that govern biometric data. Understanding the state of regulation in today's global world this section focuses on some of the most important regulations, i.e., General Data Protection Regulation (GDPR) in the European Union, California Consumer Privacy Act **(**CCPA) in the United States of America and Personal Data Protection Bill **(**PDPB) in India.

2.1. The General Data Protection Regulation– European Union

The current GDPR implemented on May 25, 2018, is regarded as one of the most protective and strong data protection laws across the world. It lays down stringent guidelines regarding what happens to personal data including biometric data and about how we bring about clarity concerning the handling of those data because of transparency, accountability and individual rights. The GDPR is meaningful because it covers not only businesses in the European Union but also any company that manages EU residents' data.[10]

GDPR reserves a special place for biometric data as this type of data belongs to the list of special categories of personal data. This encompasses data that are employed in identification of a person by use of a reference number like a fingerprint, facial point or iris scan.

[10] General Data Protection Regulation (GDPR), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, art. 9, 2016 O.J. (L 119) 1, 4, *available at*: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (last visited on March 03, 2025).

The biometric data can only be collected and used where the person has provided clear and specific consent and robust data protection laws globally. It sets a high standard for how personal data, including biometric data, must be handled, with an emphasis on transparency, accountability, and the protection of individuals' privacy rights. The GDPR .is significant because it applies not only to organizations within the European Union but also to any organization processing the personal data of EU residents, regardless of the organization's location. Under the GDPR, biometric data falls under the category of special categories of personal data, which are subject to stricter rules. This includes data used for uniquely identifying a person, such as fingerprints, facial features, or iris scans. Article 9 of the GDPR explicitly states that the processing of biometric data is prohibited unless certain conditions are met, such as:

i. Individuals must give their clear and specific consent for the collection and use of biometric data. This consent must be rational, and voluntary and it cannot be forced.
ii. Sometimes biometric data may be processed to fulfil contractual liability as well as to abide by legal requirements.
iii. Biometric data may only be processed when this is essential for somebody's life or bodily integrity.
iv. Biometric data may also additionally be processed where required in the public interest, for example for reasons of law enforcement or national security, but such processing can only occur where it complies with other relevant legal measures. data, including biometric data, must be handled, with an emphasis on transparency, accountability, and the protection of individuals' privacy rights.

The GDPR is significant because it applies not only to organizations within the European Union but also to any organization processing the personal data of EU residents, regardless of the organization's location. The GDPR ensures individuals' rights over their biometric data.[11] These rights include the right to access, rectify, erase (right to be forgotten), restrict processing, and data portability.[12] Individuals also have the right to

[11] *Id.*, art. 10.
[12] *Supra* note 10, art. 15-21.

withdraw their consent at any time, which means that organizations must have mechanisms in place to ensure that individuals can easily exercise their rights.

2.2. California Consumer Privacy Act (CCPA) – United States

The CCPA is one of the most intrusive data protection laws in the United States that operates since January 1, 2020. Although the CCPA does not directly categorise biometric data as personal identifiers on its own, the law protects biometric data as part of information that is personal. CCPA regulate companies, which act as businesses and comply with some predefined criteria, such as obtaining gross revenue of $25 million or more or selling the personal information of 50000 or more California residents. This requires organizations to inform individuals on the sort of personal information being collected particularly biometric information and the reasons for collection in United States. While the CCPA does not specifically single out biometric data, it addresses it under the broad definition of personal information, which includes biometric identifiers such as fingerprints, facial recognition, and voice recordings.[13]

The CCPA applies to businesses that collect personal information from California residents and meet specific thresholds, such as having gross revenues of over $25 million or collecting personal data from 50,000 or more consumers. Under the CCPA:

i. Businesses are required to disclose the types of personal information they collect, including biometric data, and the purposes for which it will be used. This is part of the notice at collection requirement.
ii. The CCPA grants California residents specific rights, including the right to know what personal information is being collected, the right to access and delete that information, and the right to opt out of the sale of their data. This extends to biometric data, which means that individuals can request access to their biometric data, request its deletion, or opt out of its sale to third parties.
iii. The CCPA emphasizes that data should only be collected for specific, legitimate purposes. Organizations must not retain biometric data for longer than necessary for those purposes.

[13] California Consumer Privacy Act, Cal. Civ. Code, 2018, s. 1798.100.

iv. The CCPA includes provisions that prevent businesses from discriminating against consumers who exercise their rights, such as by denying them services or charging them higher prices.

While the CCPA recognizes biometric data as personal information, it does not impose the same stringent requirements as the GDPR in terms of special treatment for sensitive data. However, it still grants consumers significant control over the collection and use of their biometric data.[14]

In 2023, the CPRA amended and expanded the CCPA, further strengthening privacy protections. Under the CPRA, biometric data remains subject to the same rules but with additional consumer rights, such as the right to correct inaccurate personal information and expanded enforcement powers for the California Privacy Protection Agency (CPPA).

2.3. India's Personal Data Protection Bill (PDPB)

PDPB is a robust data protection regulation that exists in India and is awaiting some final touches that should allow it to be ratified shortly. The bill is based on the GDPR, and its main goal is to respond to the challenges connected with the protection of personal data, including biometric data, collected, processed, and stored through devices installed in the Bulgarian territory.[15]

Under the PDPB, biometric data is classified as sensitive personal data (SPD), along with other types of personal data such as financial information, health data, and sexual orientation. Sensitive personal data is subject to more stringent processing conditions compared to general personal data. The processing of biometric data is allowed only when:

i. The PDPB requires explicit consent from individuals before their biometric data can be collected or processed.
ii. The PDPB allows the processing of biometric data for purposes such as providing services to the individual, ensuring security, and fulfilling legal obligations. However, the processing must align with specified purposes and cannot be used beyond what is necessary.

[14] *Ibid.*
[15] Personal Data Protection Bill, 2019 (Bill No. 373 of 2019), s. 2(y).

iii. Organizations that process biometric data are required to conduct Data Protection Impact Assessments (DPIA) to identify and mitigate risks associated with such data processing.

iv. The PDPB mandates that sensitive personal data, including biometric data, be stored and processed within India, although certain exceptions exist for cross-border data transfer under specific circumstances. The bill also requires the implementation of strong security measures to protect biometric data from unauthorized access, theft, and misuse.

v. PDPB proposes the creation of a Data Protection Authority (DPA) to oversee compliance with data protection regulations and to investigate complaints regarding data processing practices, including those involving biometric data.

2.4. Challenges and Considerations in the Regulatory Landscape

Biometric technologies are undergoing a period of rapid expansion in terms of their use and applying laws and regulations. Biometric technologies are living objects that require constant updating since there are newer technologies that are already in the market such as AI based biometric systems and facial recognition systems whose issues of efficacy, fairness and privacy are emerging constantly.

They also posted that there are legal differences to regulation of biometric data in different countries, thus becoming a challenge to organizations with a global presence. The individuals' privacy and rights, several challenges need to be addressed:

i. Biometric technologies are continuously evolving, and regulations must keep pace with new developments, such as AI-powered biometric systems and facial recognition technologies that raise unique concerns regarding accuracy, bias, and privacy.

ii. Different countries have varying approaches to biometric data regulation, and this creates challenges for organizations that operate internationally. Firms face a matrix of laws that can be contradictory in this area although there are some common principles observed, especially concerning cross-border data transfers and employment of biometric data for security purposes.

iii. For biometric systems to be widely used acceptance by the public is mandatory living. While the GDPR, CCPA, and PDPB offer robust frameworks for

protecting individuals' privacy and rights, several challenges need to be addressed.

iv. Biometric technologies are continuously evolving, and regulations must keep pace with new developments, such as AI-powered biometric systems and facial recognition technologies that raise unique concerns regarding accuracy, bias, and privacy.

v. Different countries have varying approaches to biometric data regulation, and this creates challenges for organizations that operate internationally. Companies must navigate a patchwork of laws that may have conflicting requirements, particularly when it comes to cross-border data transfers and the use of biometric data for surveillance purposes.

vi. Public trust in biometric systems is essential for their widespread adoption. Those regulatory frameworks must include provisions where people are uncomfortable and fear that biometric data will be used for monitoring or tracking without, their consent so that the use of these systems will be perceived as safe.

Currently, it has not yet been established by which global regulations for the use of biometric technologies are to be governed; however, the GDPR, CCPA, and the PDPB are critical foundations in the proper handling of biometric data based on the rights of the individual. Although such regulations are already in place, it is necessary to pursue continued improvement of the regulation to solve new problems including biometric surveillance, data leakage, and algorithm bias. Biometric regulation of the future implies several questions concerning technology implementation, privacy, and human rights protection.

3. Implications of Biometric Technologies

The good in this case might be argued as more security, better efficiency, and numerous other advantages that biometric technologies fill in across sectors. Yet, ethical concerns concerning projection bias, anonymity, and erosion of public trust tag along. They provide chosen problems to be addressed from many fronts which harmonize technology and safeguard individual rights.

Some social issues related to biometric systems involve the threat of bias and discrimination from algorithmic bias. Most face recognition technologies typically rely

on machine-learning algorithms trained on huge datasets. Still, these datasets are not representative in the same manner for all people. An algorithm that was mainly trained using photographs of one demographic could work exceptionally well for that population but will completely fail in the face of images representing non-dominant groups. The outcome can readily result in either rare false positives or false negatives among the minorities, and therefore, the potential for discrimination. Such biases significantly agitate precision and equity, primarily against vulnerable groups. The algorithms' reproduction of prevalent social biases does not mitigate the latter; instead, under many circumstances, the partial mitigation of prevailing socioeconomic disparities within the procedures becomes a social injustice.[16] The risk of algorithmic bias in biometric systems remain only because of technical or hardware-induced problems and soon raises critical questions of no less than ethical kind.

By design, biometric systems are, meant to automate identification and verification processes, hence often evading the oversight of a human.[17] Still, if these systems are based on fundamentally flawed or highly weak diversified data, then they shall certainly promote, and potentially thrive upon, discriminatory practices and the consequences would include utterly unequal treatment to marginalized communities in law enforcement, health care, and employment. For example, members of racial minorities are most probably misidentified by the facial recognition systems used during the policing process and that may in turn result in false accusations or arrests. Such cases question issues of accountability and integration as concerns for developing and using biometric technologies.

If not appropriately scrutinized, such systems can end up working as discriminative tools rather than equalizers. Another ethical issue that is linked to the use of biometric technologies is the right to anonymity. As the usage of biometric technology continues to grow in society, people cannot enjoy full privacy in public anymore.[18] Contrary to the numbers used in passwords and ID cards, biometric templates comprising

[16] Emilio Ferrara, "Fairness and Bias in Artificial Intelligence: A Brief Survey of Sources, Impacts and Mitigation Strategies" 6(1) *Sci* 3 (2024), *available at*: https://doi.org/10.3390/sci6010003 (last visited on March 03, 2025).

[17] Office of the Victorian Information Commissioner, "Biometrics and Privacy: Issues and Challenges", *available at:* https://ovic.vic.gov.au/privacy/resources-for-organisations/biometrics-and-privacy-issues-and-challenges/ (last visited on March 05, 2025).

[18] Kate Crawford, "Artificial Intelligence's White Guy Problem" *N.Y. Times,* June 25, 2016.

fingerprints, facial patterns, and voice patterns are original and unique as well as cannot be changed. Once captured, this information can be followed from one domain to another, such as in the case of social networking platforms and surveillance systems, and with the consent of the owner. This relates to the following ethical issues: personal freedom, autonomy, and civil liberties are highly valuable in society though their infringement appears to be increasing through the infringement of anonymity.

The use of biometric technologies would deny them this right thereby increasing the chances of a surveillance society where people's movements and behaviours are recorded. Under such conditions, people may refuse to act or speak out loud or engage in activities that require them to step out of the social norms they spot as abettors focus on them. This is an alarming development for any democratic nation since freedoms of expression and the ability to protest are cornerstones of any democratic society. The public surveillance environments where biometric devices are used for identification or tracking for which an individual's permission has neither been sought nor obtained is where the emergency and security concerns are most strongly felt. In such cases, free speech fair trials and press freedom are restricted for the consideration of security, freedom of press and freedom of speech restricted in the name of security questions have therefore arisen.[19]

There is another factor that is very key in the manifestation of biometric technologies, this is the confidence that people have in the innovations. For these systems to work appropriately, people must trust that their data shall be safeguarded appropriately. In today's world, people care about their privacy and the handling of their data, they worry about data breaches and algorithms that may be biased, and they do not want the system to go wrong. That is especially the case in industries where errors in identification and data abuse can cause significant harm, especially, healthcare and law enforcement industries. believe that data will be handled responsibly and securely. Widespread concerns over privacy, data breaches, and algorithmic bias will erode public trust and make people less willing to engage with or accept biometric technologies in their daily lives. This is particularly so in sensitive sectors such as healthcare and law enforcement, where the consequences of misidentification or data misuse can be severe.

[19] Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification" 81 *Proceedings of Machine Learning Research* 1, 3–5 (2018).

Biometric systems must be trusted by the public to perform their tasks and protect biometric data; people must be informed about how biometric information is utilized.[20] This way, accepting individual control and letting them decide whether or not they want to be enrolled in biometric systems or making sure they have access to information about how exactly their data is being stored and shared goes a long way in creating acceptance of this system as being ethically correct. For instance, if the citizens are engaged in conversations such that they understand and are comfortable with the implication of having either a biometric, an opt-in or an opt-out system particularly true in sensitive sectors such as healthcare and law enforcement, where the consequences of misidentification or data misuse can be severe.

This means building public trust in biometric systems through transparent data protection, strong data protection, and communication to the public regarding how their biometric data is being used. Making sure that the individual is in control of his data, whether through opt-in or opt-out options on biometric systems or granting access to information on the storage and sharing of one's data, would be an important step in building public trust. Engaging communities in conversations regarding the ethical implications of biometric technologies may also help build acceptance and develop systems that better reflect societal values. For the achievement of a greater improvement and gaining public confidence, the ethical considerations also have to be made through the development and implementation of complete and coherent regulatory frameworks shall also be important. Such frameworks should be developed to prevent bias, corruption and abuse of rights in implementing biometric systems and respecting individual rights.[21]

Most scholars have propounded better regulatory frameworks for use of biometric technologies as the response to these ethical issues. These guidelines should set measurable best practices for collecting, storing and using of biometric data and at the same time, guarantee non-discriminatory bias of these systems. The policy makers must collaborate with the technologist, ethicist and other civil society stakeholders emerging around the world to generate ways and means of safeguarding the rights of individuals while at the same time addressing the concern on how biometric technologies shall only

[20] Clare Garvie Alvaro Bedoya, *et. al.*, "The Perpetual Line-Up: Unregulated Police Face Recognition in America", Georgetown Law Centre on Privacy & Technology (October 18, 2016), *available at*: https://www.perpetuallineup.org/ (last visited on March 05, 2025).

[21] Megan Graham, *Building Public Trust in Biometric Technologies*, 24 Data Privacy L. Rev. 135 (2022).

be used appropriately. Periodic review of biometric systems can remove prejudice in it while clear policies on how the data collected is utilized would ensure that people remain in charge of their data.

Also, this culture of ethical norms in developing technology must be continued to avoid the future consequences of which biased or discriminative practice will become acceptable. Here, the developers and stakeholders have to be able to prevent and solve ethical dilemmas when they arise. Since the focus is on ethical concerns related to the development of biometric systems in organizations, their benefits are indeed open to everyone involved and not for the privileged few. Beyond basic questions regarding fairness and privacy compromises afforded by algorithmic systems, subsequent questions of ethics can be asked that relate to individual and social norms and values.[22] For example, the growth of the physical identification of many public places and the enveloping of apartments by the technology of biometric identification lead to a condition of fear and mistrust among people and prevent free expression of interests and disturbance of social cohesion.

The technology being questioned is entering other domains of social life sufficiently to be deemed worth examining various effects it could have on society and to ensure that the use of biometric systems does not curtail specific rights, such as freedom of speech and the right to privacy. The handling of these ethical challenges is not a mere technicality but rather an intended moral proposition. More and more societies today rely on biometric technologies and hence there is a call to shape these systems in such a way that they can support the provisions of social justice and equity. This means dedication toward using biometrics as a means of developing technologies that add value to the lives of those who use them, most importantly, members of society who have always been discriminated against. Therefore, involving the voices of different people, and organizations can prevent bias and enshrine fairness to biometrics are promising yet raise substantial ethical issues regarding algorithmic bias the right to anonymity and public trust.[23] These problems can only be solved by the appropriate legislation, involving the public and respecting the principles of ethical innovation. Concern for fairness,

---

[22] Omer Tene and Jules Polonetsky, "Privacy in the Age of Big Data" 64 *Stanford Law Review* (February, 2012), *available at:* https://www.stanfordlawreview.org/online/privacy-paradox-privacy-and-big-data/ (last visited on March 05, 2025).

[23] Shoshana Zuboff, *The Age of Surveillance Capitalism* 320 (PublicAffairs, 2019).

accountability and transparency means that societies will be able to realize benefits from biometric technologies while at the same time ensuring that citizens' rights and the use of technologies do not infringe on other's rights.

4. Biometric Data and Intellectual Property

The advent of biometric technologies has changed the face of identification and authentication, bringing in new challenges and considerations about ownership, control, and the ethical implications of these technologies in our increasingly digital society. Biometric data, which includes unique identifiers such as fingerprints, facial recognition patterns, and iris scans, has become integral to various applications from security systems to personal identification. As these technologies unfold into the mainstream, it is critical to understand the jurisdictional and intersections with intellectual property rights of such biometric data.[24]

As can be inferred, classification of intellectual property in the case of biometric data is complex and multidimensional. The traditional intellectual property regimes generally guard creations of the mind that include inventions, designs, trademarks, and copyrights. On the other hand, biometric data involves human identities and, consequently, cannot reside in that traditional framework. As is depicted on one hand, it follows that a person's private biometric information belongs to the person due to its unique biological and behavioural characteristics. On the other hand, who owns it raises further ambiguity.[25]

The biometric data is usually collected by the government and private companies for different purposes, such as law enforcement, security, and marketing. The situation raises crucial concerns over consent, ownership of data, and potential misuse. It is therefore necessary to examine the balance between individual rights and societal interests in owning and controlling biometric data. Culture of ownership of biometric data is patented by the organizations that manage and preserve such data rather than the people to whom these data relate to.

The laws and regulations are often insufficient in many countries for the protection of rights of individuals concerning biometric information; business say and

[24] *Supra* note 17.
[25] *Ibid*.

governments characterize the biometric data as a material for earning money or for the purpose of monitoring of people. For instance, where individuals offer their biometric data to be used in identity verification in such nationhood initiatives, are they able to control further use of the same data.[26]

The fault of losing control is something that can be costly when it comes to privacy and civil liberties. When biometric technologies are invested into more societal functions, people find themselves observed or controlled for with their consent.

Additionally, it illustrates that the lack of juridical identity of biometric data can even deepen these problems and create gaps in protection. Privacy and data rights continue to be an active debate, therefore there is a need for a strong solution that protects the ownership and control of biometric data in order to promote rights of the individuals. By doing so it can be deduced that the use of intellectual property in the protection of biometric technologies is a double edged sword. The patents stimulate creativity because inventors gain protection for their idea, which is the invention. This protection fuels the development of the biometric technologies to improve and optimize the security performance and the level of satisfaction of the customers.

The patenting of biometric technologies, such as facial recognition algorithms or fingerprint scanning systems, has led to significant strides in the field, fostering competition and investment. Companies and researchers are more likely to develop new applications and improve existing technologies when they know their innovations will be protected from unauthorized use.[27] This can lead to rapid technological progress and a wide range of biometric solutions that make things easier and more secure for different industries, such as finance, healthcare, and law enforcement. For instance, biometric authentication methods, like fingerprint scanning for mobile devices, have greatly simplified access while enhancing security measures.

The rising commercialization of biometric technologies has led to many ethical questions, mainly over privacy and security in the management of data. The fight to secure patents on newly developed biometric innovations pushes companies toward more profits, potentially leading them to neglect other aspects related to ethics. This struggle is

[26] Daniel J. Solove, *Understanding Privacy* 42–46 (Harvard University Press, 2008).
[27] *Ibid*.

evident with facial recognition technology, an application whose benefits greatly outweigh the negatives but one that may still impinge upon personal privacy and civil liberties.[28]

The lack of proper controls for facial recognition technologies deployment has led to rampant surveillance and the breaches of personal data and misuse. Some wrong arrests based on mistaken identities demonstrate what can go wrong with improperly controlled facial recognition technologies. There is also the risk of the potentially discriminatory nature of these systems, as algorithms can perpetuate or amplify present-day inequality in society.

This requires stronger regulations and higher ethical standards in the use of biometric technologies. Policymakers must balance the promotion of innovation through intellectual property protections against the need to protect individual rights, ensuring that privacy and ethical standards are maintained. This calls for a review of existing intellectual property frameworks regarding the specific features of biometric data and its connection to personal identity.[29] This could potentially lead to another significant issue associated with the intersection of biometric data and intellectual property. The relationship of biometric data with intellectual property is very complex and raises issues with ethical concerns. Ownership and control of biometric data raise considerable questions about rights of individuals as well as misuse by governments and private entities. Incentivization of innovation in biometric technologies through intellectual property laws carries the risk to privacy and civil liberties if the same are not implemented along with proper safeguards.

This would, therefore, be a matter of developing an appropriate legal framework that balances the need for innovation with the imperative to protect rights and privacy. That calls for dialogue between lawmakers, technologists, ethicists, and the public about

[28] Ravi K. R., "The Rising Use of Surveillance Technologies in Law Enforcement: A Double-Edged Sword", *available at:* https://www.intelegal.in/the-rising-use-of-surveillance-technologies-in-law-enforcement-a-double-edged-sword (last visited on March 06, 2025).

[29] Sammed Akiwate and Gagandeep Kaur, *et.al.*, "Facial Recognition Technology & Legal Implications in India: An Analysis", in Kanchal Gupta and Rupendra Singh, *Law & Technology: New Perils in Justice and Accountability* 240 (Red'Shine Publication, 2023).

what the deployment of biometric technologies should mean in light of societal values and principles.[30]

Ultimately, building more equitable and ethical ways of handling biometric data will enhance public trust and foster responsible innovation in this increasingly cutting-edge field. The incorporation of ethical considerations within biometric development and deployment will ensure that these technologies empower rather than violate human rights.

This approach requires interdisciplinary coordination, where legal frameworks, technological progress, and ethical considerations need to be aligned. It is through such collaborative efforts that the societies can navigate the complexities of biometric data and intellectual property and utilize these powerful technologies responsibly for the greater good.[31]

5. Privacy and Data Security Concerns in Biometric Technologies

Biometric technologies capture and analyze unique physical or behavioral traits, such as fingerprints, facial features, iris scans, and voice patterns. Biometrics are spreading over a vast number of areas from security services to healthcare and finance. Although biometric technologies can increase convenience, personalization, and security, they have vast privacy and security concerns related to data. This is mainly because the nature of biometric data is extremely sensitive in that once compromised, they will have irreversible results.

Biometric data is usually obtained through devices like fingerprint scanners, facial recognition cameras, or iris scanners. Unlike passwords or PINs, biometric data cannot be changed once compromised; therefore, it is particularly sensitive personal information.[32] Understanding how biometric data is stored, processed, and used is central to grasping the privacy and security risks.

When biometric data is collected, it is often stored in digital form. Most systems do not store the raw biometric data but rather create a mathematical template or biometric signature that represents the unique features of an individual. For example, in facial

[30] Shivangi Gaur, "Safeguarding Biometric Data as Intellectual Property in the Age of AI", *available at*: https://lexprotector.com/blog/safeguarding-biometric-data-as-intellectual-property-in-the-age-of-ai/ (last visited on March 10, 2025).

[31] Julie E. Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* 174–178 (Yale University Press, 2012).

[32] John D. Woodward, Nicholas M. Orlans, *et. al.*, Biometrics 54-56 (Mcgraw-hill, 2003).

recognition, the system may extract key facial landmarks such as the distance between the eyes or the shape of the nose and store these in a template form. Similarly, fingerprint scanners typically store a set of numerical representations based on ridge patterns.

However, the process of raw biometric data transformation into a template does not reduce privacy risks. These templates, although not containing the raw image or data, are highly unique to an individual and may be reverse-engineered or matched against other databases. In addition, unsecured storage systems used for holding biometric templates make them prime targets for hackers.[33]

The algorithms process the collected biometric data in verification or identification of the person. This occurs when a fingerprint of an individual is scanned and then matched with a database of stored templates to identify or verify his identity. Matching of the biometric data may happen locally on the device such as a fingerprint scanner or even at a remote location, with data transmitted over the network to a central server for processing.

In the case of remote processing, the risk of interception is very high, especially when unsecured networks are used in transmitting sensitive biometric data. This may lead to an unauthorized access, modification, or misuse of the data at the time of transmission, a critical concern when dealing with highly personal information like fingerprints or facial recognition data. Biometric data is sensitive and unique, and therefore a prime target for cybercriminals. The risks of hacking or unauthorized access to biometric databases are substantial, as any breach of such data would have long-lasting consequences for both individuals and organizations.

The security threats posed to biometric databases are not different from any other digital system. In 2019, for example, over 1 million people had their personal biometric data exposed through a massive data breach. The breach resulted from weaknesses in a biometric fingerprint identification system employed by various organizations. This breach was not limited to the biometric data, rather, it involved personally identifiable information such as names, phone numbers, and email addresses.

[33] Afifa Fatima, "Legal and Ethical Issues of Biometric Data and Aadhaar in India", Law Juirst (June 22, 2024), available at: https://lawjurist.com/index.php/2024/06/22/legal-and-ethical-issues-of-biometric-data-and-aadhaar-in-india/ (last visited on March 10, 2025).

Once hackers gain access to biometric data, they could use it for identity theft, fraud, or other malicious activities. Unlike passwords, which can be reset, compromised biometric data cannot be easily changed. If a person's fingerprint or facial features are exposed, there is no way to reset these attributes, leaving the individual permanently vulnerable to identity theft.[34]

The second risk is the possibility of insider threats where employees or people with authorized access to biometric data misuse their access for malicious purposes. For instance, an ill-trained or unscrupulous employee may misuse the biometric data for unauthorized surveillance, stalking, or other unethical purposes. As such, organizations handling biometric data must ensure strict access control measures and comprehensive auditing mechanisms to prevent unauthorized access.

Many organizations store biometric data in central databases, which are often provided by third-party service providers. This would make these databases prime targets for cybercriminals in case they are not sufficiently protected.[35] For instance, the facial recognition data, being stored in cloud servers, might be accessed or stolen, with chances of misuse. With advancements in artificial intelligence and machine learning, the stolen biometric data could be manipulated to produce synthetic biometrics, thus creating a more complex situation.

Anonymization is a technique that involves transforming data in such a way that it can no longer be linked to a specific individual without the use of additional information. For many types of personal data, anonymization can provide a level of security and privacy protection, as it ensures that the data cannot be traced back to the individual from whom it was originally collected. Nevertheless, anonymization is not completely effective, especially in the case of biometric data. The significant problem with the anonymization of biometric data is that it is inherently personal and identifiable.

Even if the Personally Identifiable Information (PII) is removed from biometric templates, an anonymized biometric dataset is susceptible to re-identification using advanced techniques.[36] Certain biometric templates, like facial recognition data, have

---

34 Anil K. Jain, A. Ross, *et. al.*, "An Introduction to Biometric Recognition", 14(1) *IEEE Transactions on Circuits and Systems for Video Technology*, 4-6 (2004).

35 *Ibid.*

36 Marc Rotenberg, Jeramie Scott, *et. al.*, *Privacy in the Modern Age: The Search for Solutions* 75-77 (The New Press, 2015).

been shown by researchers to be re-identifiable with a very high degree of accuracy against massive databases or even using AI-powered re-identification algorithms. Furthermore, biometric data can be used in combination with other non-anonymous data, such as location information or personal records, to pinpoint an individual's identity.[37] Thus, anonymization techniques traditionally used in other contexts may not be so effective when dealing with biometric data.[38] Pseudonymization - the replacement of identifiable information with pseudonyms - reduces privacy risks but also involves some risks, especially when used in conjunction with other databases.

Some of the biometric systems are trying to anonymize the data by processing it locally on the device, which doesn't send the raw biometric data or templates over to the external servers. In such cases also, some kind of anonymized template may be stored on the system for future usage, which may again get traced to the same person, if the data is detailed. As biometric technologies improve, the ability to anonymize biometric data in a way that prevents identification becomes increasingly difficult.[39]

To address privacy and data security concerns, organizations need to adopt a comprehensive set of best practices for handling biometric data. These practices include:

i. Encrypting biometric data both in transit and at rest is essential to ensure that even if data is intercepted, it remains unreadable without the appropriate decryption keys.

ii. Whenever possible, biometric data should be processed locally on the device rather than transmitted to centralized servers. This reduces the risk of data interception and hacking during transmission.

iii. Strict access control measures should be implemented to ensure that only authorized individuals have access to biometric data. Role-based access controls and multi-factor authentication (MFA) can further enhance security.

---

37 *Supra* note 34.
38 *Ibid*.
39 Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization", 57 *UCLA Law Review* 1701, 1703 (2010).

iv. Continuous monitoring and regular audits of biometric systems can help detect any unauthorized access or anomalies in data processing activities. This ensures that breaches or violations are promptly identified and addressed.

v. Organizations should obtain explicit consent from users for the collection and processing of biometric data. They should also be transparent about how the data will be used, stored, and shared.

The biometric data has significant potential to enhance security, service efficiency, and the experience of users. Its nature has made it uniquely susceptible to privacy breaches and data breaches. The storage, processing, and sharing of biometric data need to be managed properly to avoid the risks of hacking, unauthorized access, and misuse. Additionally, anonymization, as a concept, is helpful but does not have much application in biometric systems as the inherent risk of re-identification cannot be avoided.[40] Therefore, robust security practices, strict data governance policies, and comprehensive regulatory frameworks must be in place to protect biometric data and ensure that privacy and data security concerns are tackled accordingly. As biometric technologies evolve, the tension of innovation with privacy will forever remain a critical issue at play.

6. Informed Consent and Public Awareness in Biometric Data Collection

Biometric technologies have become a cornerstone in modern security, identification, and personalized services, ranging from fingerprint scans and facial recognition to voice identification and iris scans. As these technologies continue to integrate into daily life, ensuring the informed consent of individuals whose biometric data is being collected has become a fundamental issue. Informed consent is agreed to when one understands precisely what personal data or biometric data is to be collected, how it is going to be used, and the risks that might arise with its processing.[41] This section discusses the importance of informed consent in the context of biometric data collection, explores how various jurisdictions require organizations to obtain such consent, and

[40] *Supra* note 37.

[41] Shravishtha Ajay Kumar, "Ethical and Regulatory Considerations in the Collection and Use of Biometric Data", *available at:* https://www.orfonline.org/research/ethical-and-regulatory-considerations-in-the-collection (last visited on March 11, 2025).

highlights the challenges of ensuring public awareness about the implications of providing biometric data.

Informed consent is the foundation of ethical practice in medical and non-medical environments. It ensures that individuals have all the information they need to make an autonomous, informed decision regarding their participation in activities that involve the collection, processing, or sharing of personal data.[42] In the case of biometric data, informed consent is the process of fully informing individuals about the following:

i. Individuals must understand which specific biometric data will be collected, whether it is fingerprints, facial recognition, iris scans, or other biometric identifiers.

ii. Individuals must know why their biometric data is being collected. Whether it is for security purposes, user authentication, personalization of services, or surveillance, transparency regarding the purpose is crucial.

iii. People must be informed about the intended use of their biometric data, including how it will be processed, stored, and analyzed. This includes details about any third parties involved in processing or accessing the data.

iv. Individuals should be informed about how long their biometric data will be stored and the conditions under which it will be deleted. Retention policies are critical, especially when dealing with sensitive data.

v. As biometric data is immutable, unlike passwords, which can be changed, individuals need to understand the risks involved in providing their biometric data. If this data is exposed or misused, it cannot be reset or replaced, making it particularly vulnerable to identity theft, fraud, or surveillance.

vi. Individuals should also be informed about their right to withdraw consent at any time and the consequences of doing so, including how this will affect their ability to use certain services.

Biometric data, by nature, is deeply personal and unique to individuals, making its collection a sensitive issue. Unlike other forms of data, such as usernames or email addresses, biometric identifiers are permanently tied to an individual's physical traits. The

[42] *Ibid.*

risks of misuse or theft of this data are significant, and once compromised, biometric information cannot be reissued or changed, making robust, informed consent processes necessary.[43]

Informed consent protects the privacy and autonomy of individuals by ensuring that they are doing something in full knowledge of how information about them will be utilised. It is likewise a protection for the institutions, which ensures compliance of legal and ethical obligations while minimizing the dangers of lawsuits or regulatory violations.[44]

Moreover, the absence of informed consent can lead to trust issues between individuals and the entities collecting biometric data. For instance, if individuals are not fully informed about how their biometric data is being collected and used, they may feel violated or exploited, leading to public backlash and loss of business for organizations.

6.1. Global Jurisdictions and Consent Requirements

The legal frameworks in different jurisdictions around the world vary in terms of how they govern the collection of biometric data and the requirement for informed consent. These frameworks are designed to balance the benefits of biometric technology with the need to protect individual privacy and human rights. The various provisions how informed consent is handled in some key regions are mentioned below:

6.1.1. European Union

The GDPR of the European Union is one of the most comprehensive data protection laws in the world. It considers biometric data as special category data because it is sensitive. The GDPR requires organizations to obtain explicit, informed consent from individuals before collecting their biometric data.[45]

Article 9 of the GDPR specifically addresses the processing of special category data, including biometric data.[46] For consent to be valid, it must be:

i. Consent should be given voluntarily, without any coercion.

[43] *Supra* note 41.
[44] *Ibid.*
[45] *Supra* note 10.
[46] *Supra* note 10, art. 9.

ii. Consent must relate to a specific purpose or set of purposes for which the data is being collected.

iii. Individuals must understand what biometric data is being collected and how it will be used.

iv. Consent should be clear and given through a statement or affirmative action, such as ticking a checkbox.

The GDPR further requires that organizations provide accessible information to individuals about the processing of their data, such as the risks involved in such processing.[47] The rule also allows an individual the right to withdraw consent to such processing at any point, with equal ease compared to giving consent.

6.1.2. United States

The landscape is different in the United States due to states enacting various laws and regulations concerning consent. For example, in California, its version, the California Consumer Privacy Act, affords every California consumer the right to opt out of selling of their personal information, such as biometric information. It is also obligated upon businesses to inform consumers regarding what kind of information will be gathered, used, or shared.[48]

The Illinois Biometric Information Privacy Act is one of the most popular state-level regulations in the U.S. It has set strict standards for organizations collecting biometric data, which include getting informed consent from the individuals before collecting such data. Businesses are also required to draft a written policy on the retention and destruction of biometric data, which describes how long the biometric data will be retained and when it will be disposed of in a safe manner.[49]

Whereas the EU's GDPR provides a homogeneous norm for biometric data consent across countries, the USA provides no uniform standard for obtaining consent over biometric data, thus complicating their rights cross-jurisdictionally.

6.1.3. India

[47] *Ibid*.
[48] *Supra* note 13.
[49] Illinois Biometric Information Privacy Act, 740 ILCS 14/1 (2008).

India's Personal Data Protection Bill, currently under review, provides a provision about the biometric data of individuals as sensitive personal data. Explicit consent has been required for collection and processing. The bill does mandate that people should be informed of the purpose, scope, and usage of their biometric data and be granted the right to withdraw consent from the said data.[50]

PDPB mandates organizations to reasonably assure protection of biometric data. Clear policies for retention and deletion shall be in place. People have a right to view their data and correct/erase it as necessary. Again, as in the rest of the world, emphasis on consent is a global best practice, but one does need to worry about the effective enforcing of those rights and possible misuse.

6.1.4. China

Unlike Western data protection frameworks, China's approach to biometric data is less protective of individual rights, although it does require some form of consent under its Personal Information Protection Law (PIPL). The law mandates that individuals be informed about the collection and use of biometric data, but it is less stringent than the GDPR and does not emphasize the need for explicit, freely given consent.[51]

6.2. Challenges in Ensuring Informed Consent

While many jurisdictions have laws that address informed consent for biometric data collection, several challenges remain in ensuring that individuals fully understand the implications of providing their biometric information:

i. Many individuals may not be aware of how their biometric data is being collected, stored, or used. For instance, facial recognition technology is increasingly being deployed in public spaces, such as airports and shopping malls, where people may not have the opportunity to opt out or even be informed about its use.

ii. Consent forms and privacy policies are often written in complex legal jargon that is difficult for the average person to understand. This makes it harder for individuals to make fully informed decisions about whether to provide their biometric data.

---

[50] *Supra* note 15.

[51] Personal Information Protection Law of the People's Republic of China, Order No. 84 (promulgated by the Standing Comm. Nat'l People's Cong., Aug. 20, 2021, effective Nov. 1, 2021)

iii. In many cases, people are forced to provide biometric data to access services, such as unlocking their phones or passing through security at airports. In these situations, individuals may feel pressured into giving consent, which may not be entirely voluntary.

iv. Many organizations do not provide clear and concise information about how biometric data is used, who it is shared with, or how it will be protected. Without this transparency, individuals cannot make informed decisions about the risks of sharing their data.

v. Even when individuals are informed about their right to withdraw consent, the process may not always be straightforward. Some organizations may make it difficult to revoke consent, especially in situations where biometric data is linked to access to essential services.

Informed consent is an important aspect of collecting and processing biometric data. This ensures that people know what they are getting themselves into by providing such sensitive information. While different jurisdictions around the world have enacted legal frameworks to require informed consent, challenges remain in ensuring that people are aware of the risks involved and the full extent of data use.[52] To overcome these challenges, organizations must prioritize transparency, simplify consent processes, and empower individuals to make autonomous decisions about their biometric data. As biometric technologies continue to develop and grow, strong practices in informed consent will remain key in safeguarding privacy and ensuring public trust is not misplaced.

7. The Disproportionate Consequences of Biometric Surveillance

Biometric surveillance technologies have transformed industries, from security and policing to even health care, but their applications raise crucial issues, particularly when it comes to vulnerable groups. The most vulnerable sections of society, including minorities, low-income groups, and political dissenters, are also the first to be adversely affected by the increasing trend of biometric identification systems.[53] While making life

[52] Sara Solarova, Juraj Podrouzek, *et. al.*, "Reconsidering the regulation of facial recognition in public spaces", 3 *AI and Ethics* 625-635 (2023).

[53] Malk Partners, "Facing the Risks: Biometric Data", *available at:* https://malk.com/facing-the-risks-biometric-data/ (last visited on March 10, 2025).

easier and more secure, these technologies also involve high privacy risks, burdens of surveillance, and biases that exacerbate already existing social and economic inequalities.

One of the significant issues related to biometric surveillance is that it disproportionately affects racial minorities. It has been shown that facial recognition and other similar biometric systems have biases toward races and ethnicities, causing a higher probability of wrong identification and harassment of minorities.

In a landmark study published recently by the National Institute of Standards and Technology (NIST), the use of facial recognition systems was found to have a greater rate of error in people of colour identification, specifically people being Black and Asian than white people.[54] According to their study, commercial facial recognition systems had significantly higher misidentification rates for darker-skinned women than for lighter-skinned men. This bias is attributed to the lack of diversity in the datasets used to develop these systems, which results in lower accuracy when identifying people from certain underrepresented racial and ethnic groups. For instance, in 2018, gender classification software was found to make far more mistakes in the classification of darker-skinned, female faces compared to lighter faces. It reveals an error rate of even 34% for darker-skinned women in comparison to a mere 0.8% for light-skinned males. Errors not only cause wrongful arrests and detentions but also contribute to systematic inequality by targeting communities at higher rates of surveillance-from policing, and immigration control to facial recognition technologies deployed in public domains.

Risks related to inaccurate biometric identification are very alarming for marginalized groups where misidentification can lead to racial profiling, unlawful detention, or even wrongful convictions. In the United States, for example, the risk of facial recognition-based surveillance is higher for Black individuals and evidence of such surveillance is used in law enforcement, border control, and public spaces. This has been illustrated in an incident where the Detroit Police Department offended in a facial recognition blunder, something that made them arrest a Black man for shoplifting something he did not steal. This incident sharpens the problem of unrestrained biometric scrutiny within populations already at risk from state scrutiny or police brutality.

[54] *Ibid.*

The mentioned extensive application of biometric surveillance technologies put low-income communities before a very special kind of challenge, because they often do not possess a necessary technology and tools to safely navigate the Internet. Digital divide, the ratio of people who are technologically equipped to those who are not, is also widespread among the various sensitive categories of population such as the low and fixed-income earners, those in the rural areas, and elderly people.

Biometric identification systems cannot function effectively if high-quality, consistent data are not collected. Some of them include facial recognition, fingerprint scanning, or iris scanning are largely a biometric system that people with low income background can have a hard time mastering since they will not have high end smartphones or other technologies. Thus, a lot of them have inadequate infrastructure to use the identification system effectively and, therefore, do not get the service. For instance, biometric system is a common means of identification used in many countries for giving out state services named social services, welfare payments, or government aid. This shows that if they are unable to access biometric devices and or have no Internet connection then the above groups can end up being locked out of these services.

For instance, in India, the Aadhaar system which relies on biometric identification is often criticized in instances where bodies such as the National Institutes of Health report that the system was problematic and exclusionary particularly to the most vulnerable populations. For things like government and non-government services like social welfare schemes, door to door reporting of its biometric details such as fingerprint and iris scanning from people is done. From the reports, anytime people who are wearing off their fingerprints, particularly from the elderly or aluminium population, they have problems in the authentication process that leads to a creating of delays or denial of services.

According to a 2018 study by the Centre for Internet and Society, nearly 8 million people could not access their welfare benefits because of biometric failures. This is especially problematic for those who are already marginalized and have limited access to technology, such as rural populations or the elderly.

There is a problem of lack of a proper opt-out policy for the biometric systems, or at least, other forms of identification for those unwilling to or cannot provide biometric

data. In the year 2019, Privacy International prepared a report in which it became clear that many biometric systems used in different states, including the United Kingdom and India, do not have ways to refuse the use of biometric technologies. For the low income clients such system implies having to give up their privacy in a way not to opt out of the basic services which in turn increase their vulnerability and perpetuates socio-economic exclusion.

Biometrics are being more and more adopted by governments in politically sensitive countries to monitor and assert control over population with very little regard to privacy or civil liberties. Authoritarian regimes have resorted to biometric surveillance as an instrument of suppressing dissent; restraining protest formation and, monitoring political dissidents.

For instance, Chinese authorities have installed extensive biometric monitoring systems in Xinjiang where over one million Uyghur Muslims are forced to submit themselves to an extensive monitoring as part of the larger system of repression against their ethnic group. Human Right Watch and Amnesty International have stated that the Chinese authorities have employed genetics and facial recognition methods as part of a planned government campaign against Uyghur communities. Security is fused with social scorecards, and AI tracking of residents to target individuals who are deemed unreliable or traitors and enhance the state's manipulation of populations' conduct.[55]

Likewise, in Egypt, political protests are quenched, which has required government to conduct biometric identification in public areas of activists and opponents. It was disclosed in 2020 that Egypt had placed a network of facial recognition cameras especially in the airport and governmental facilities to monitor the opposition groups. The citizens of countries and regions facing higher instability, biometric surveillance may be employed as a means of suppression and restriction occasions. Thereby making it tough for marginalized or dissenting groups to organize or express their views freely.

The introduction of biometric surveillance also raises significant privacy and security concerns because it impacts vulnerable populations. In regions where weak legal frameworks or scant regulation exist, the information and data accumulated through a

[55] Human Rights Watch, "Break Their Lineage, Break Their Roots", April 19, 2021, *available at*: https://www.hrw.org/report/2021/04/19/break-their-lineage-break-their-roots/chinas-crimes-against-humanity-targeting (last visited on March 05, 2025).

biometric system are vulnerable to potential exploitation and hacking or to unofficial sharing and use for objectives other than those of data collection. Vulnerable populations, which include mainly unschooled individuals without strong digital literacies, may lack necessary knowledge or awareness of dangers such as these.

In 2018, it was revealed that a data breach occurred within the Aadhaar system in India, where sensitive biometric information of over 1 billion people was reportedly exposed due to vulnerabilities in the system. While the breach did not result in the direct exploitation of biometric data, it highlighted the risks associated with storing large amounts of personal data, especially when stored in centralized databases with inadequate security measures. In vulnerable populations, this breach of biometric data can lead to identity theft and fraud, and there's an increased risk of surveillance, especially when the victims lack the means or knowledge of how to protect their data.

The impact of biometric surveillance on vulnerable populations cannot be ignored. As biometric technologies continue to evolve and spread across various sectors, it is critical to ensure that the systems implemented do not exacerbate existing inequalities. To mitigate the negative effects, it is essential to promote policies that:

i. Biometric systems should be tested for racial, ethnic, and gender biases, and datasets used to train these systems should be diverse and representative.

ii. Policymakers must ensure that low-income and marginalized communities have access to the technologies required to participate in biometric systems and that alternative methods of identification are available where necessary.

iii. Strong regulatory frameworks are necessary to safeguard the privacy of vulnerable populations and to prevent the misuse of biometric data. Laws should mandate transparency, provide individuals with control over their data, and guarantee opt-out mechanisms.

iv. Biometric systems must be subject to rigorous oversight to ensure that they are used ethically and responsibly. Governments and organizations must be held accountable for violations of privacy and civil rights.

Only by addressing these concerns can we create a biometric ecosystem that benefits all individuals without perpetuating inequality or infringing on privacy rights.

8. Conclusion

Thus it can be concluded that biometric technologies, such as facial recognition, fingerprint identification, and iris scanning, have made significant advancements over the past decade. Their application across various sectors, from law enforcement to healthcare, promises to revolutionize how we approach security, convenience, and personalized services. However, as these technologies evolve, so too does the responsibility to ensure they do not infringe upon privacy rights or lead to misuse. It is difficult to balance innovation in biometric technologies with protection of individual rights by considering ethical, legal, and technological factors.

Rapid development of biometric technology calls for proactive measures on privacy, security, and ethical issues in their design and development. This requires privacy by design and ethics committee development for the creation of any biometric system. Balancing innovation in biometric technologies with robust protection for individual rights requires discussion and reformulation of policy and law.

The most effective approach to balancing innovation and protection can be found in the concept of privacy by design, which was popularized by the General Data Protection Regulation of the European Union. This concept advocates for embedding privacy measures at the levels of design and architecture as part of technology design rather than including them after the product is developed.

For biometric systems, privacy by design would mean incorporating such features as privacy and security from the entire lifecycle of a biometric system, from data collection to storage, processing, and sharing. Biometric systems must collect only necessary data, furthermore, they must make use of secured methods for storing and transferring this kind of data while allowing users to retain control over their information. This can be accomplished using data minimization, a principle that allows personal data to be collected only when necessary to reach a specified purpose.

An example of this would include using data encryption to ensure biometric data is stored safely and becomes unavailable to entities other than those with authorized access. Finally, anonymization should be adopted in which biometric data is turned into non-personal identifiers which cannot link to a particular individual. However, though these measures may limit privacy risks, all biometric data; even after anonymization,

holds inherent privacy risks as these concern the uniqueness and permanence of the involved data.

Above all, ensuring transparency regarding the use of biometric data and the rights of individuals regarding their data is central to achieving privacy by design. The purpose behind the collection of data, the possible implications that may arise from handing over information, and ways to opt out or withdraw consent should be relatively easily understood by users.

The development of biometric technologies should not be driven by market forces or technological capabilities but must be guided by ethics in the research and deployment of these systems. As the use of biometric technologies becomes more widespread, so do the risks of misuse, especially in surveillance, policing, and political control. The mitigation of these risks calls for the establishment of ethics committees at the development phase of biometric technologies.

An independent ethics committee on biometric technologies would be an independent body that would be responsible for the evaluation of the ethical implications of such systems. The committee would assess potential harms, such as racial or gender bias, and recommend measures to ensure fairness and inclusivity. For instance, an ethics committee may recommend the usage of more diverse datasets that will prevent biases in facial recognition systems, thus such technologies work equally well for people of color, women, and people with disabilities. Ethics committees would also make sure that the deployment of biometric technologies is in accordance with the core human rights principles, namely dignity, autonomy, and freedom from unjust surveillance. The committee would also monitor the long-term social impacts of biometric systems, ensuring that they do not lead to widespread profiling, exclusion, or discrimination, particularly among vulnerable populations. Establishment of an independent ethics committee is critical to the idea that these systems could only be developed with deep understanding of both their potential benefits and their risks. Such committees should comprise experts in technology, law, ethics, privacy, and social justice and must engage with a wide range of stakeholders, including civil society organizations, privacy advocates, and marginalized communities.

8.1. Recommendations for Policy and Legal Reforms

Other than the use of privacy by design and ethics committees, legal and policy reforms must come into place to mitigate rising concerns of biometric technologies. The recommendations outlined below serve as an integrated approach that would put a check in the advancement of biometric systems without harming innovation.

8.1.1. Strengthening Data Protection Laws

Existing data protection laws need to be strengthened to sufficiently protect the biometric data. While important frameworks such as the GDPR in the European Union and the CCPA in the United States regulate the manner and directions in which companies can operate, they do not come without their limitations. Clearer and more effective regulation of biometric data is perhaps needed, often taking a special category of personal data under the GDPR but not specifically addressed in most jurisdictions. Policy reforms must include:

i. Explicit definitions of biometric data within data protection laws to ensure there is no ambiguity around its scope.

ii. Stronger consent requirements to ensure that individuals are fully informed before their biometric data is collected or processed, with clear, accessible mechanisms for consent withdrawal.

iii. Data retention limits, stipulate that biometric data should only be retained for as long as necessary for its original purpose, with strict guidelines on deletion.

iv. Data subject rights should be explicitly expanded to cover biometric data, ensuring that individuals have the right to access, correct, and delete their biometric information.

8.1.2. Legislative Reforms for Biometric Technologies

Legislation should be made on the use of biometric technologies, especially were applied in sensitive areas, like law enforcement, immigration, and social services. Biometric systems should not be used lightly without oversight. Some of the most important legislative changes to make include:

i. Laws should prevent the widespread use of facial recognition or other biometric technologies in public spaces without clear, justified purposes. This would help

curb intrusive surveillance, particularly in democratic societies, where privacy rights are paramount.

ii. Biometric systems should be regulated to prevent their misuse in policing. Legislation should ensure that biometric data is only used for specific, well-defined purposes, such as preventing identity theft, and should be accompanied by clear guidelines on accountability and transparency.

iii. To ensure compliance with ethical standards, biometric systems used in public spaces or by government agencies should be subject to third-party audits that assess their fairness, accuracy, and impact on privacy.

8.1.3. Public Engagement and Transparency

Public engagement constitutes an essential element in building trust in the biometric technology. Governments and institutions implementing biometric systems should make openness a priority, letting people understand how their biometric data is utilized and the risks that are associated. Public consultations among citizens, privacy advocates, and other experts in technology should be undertaken before the implementation of biometric systems in public sectors. Reforms include:

i. Governments should engage in public education campaigns to inform citizens about the implications of biometric technologies and how their data is being used.

ii. Institutions and organizations implementing biometric systems should be required to provide transparent, publicly accessible reports detailing how biometric data is collected, processed, and protected.

iii. Citizens should have access to effective mechanisms for reporting violations related to biometric data collection, as well to seek redress in cases of misuse.

8.1.4. Encouraging Innovation in Biometric Technologies

While the need for regulation and protection is clear, it is equally important to foster innovation in the field of biometrics. Encouraging responsible innovation can lead to the development of safer, more inclusive, and effective biometric systems. Governments and regulatory agencies should provide incentives in developing privacy-preserving biometric technologies, such as secure multi-party computation or federated

learning, through which biometric data are processed without ever leaving the user's device and compromising privacy. Such incentives for research and development include:

i. Governments should fund research into privacy-enhancing biometric technologies that prioritize data security and minimize risks to individual privacy.

ii. Developers of biometric systems should be encouraged to adhere to ethical standards and engage with interdisciplinary teams to assess the social implications of their technologies.

To balance innovation in biometric technologies with safeguarding individual rights, a multi-stakeholder approach is needed. This can be achieved through the infusion of privacy by design, the setup of ethics committees, and robust legal frameworks to ensure that biometric systems are both effective and respectful of privacy. Public engagement and transparency are also crucial in fostering trust and putting into use biometric technologies in ways that actually benefit society without undermining fundamental rights. With appropriate policy and legal reform, we can reap the potential of biometric technologies without impairing the dignity, privacy, and freedoms of human beings.