VOLUME 6 | ISSUE 4

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

BIOMETRIC TECHNOLOGY THROUGH TIME: A STUDY OF ITS HISTORICAL DEVELOPMENT

- Poushali Bhattacharya[1]

ABSTRACT

In today's society, the necessity to prove one's identity has become increasingly prevalent, permeating various facets of daily life. From unlocking smartphones to accessing secure venues, the need for reliable authentication methods is undeniable. Biometric identification stands as a remarkable solution in this landscape, harnessing the unique attributes of individuals' bodies, such as fingerprints or facial features, as keys to access. This concept represents a paradigm shift in security measures, as biometrics offer an unparalleled level of difficulty in replication, thereby enhancing safety and reliability. At its core, biometric authentication functions as a security mechanism predicated on the recognition of distinct physical or behavioral traits. These traits encompass a diverse range of characteristics, including facial features, iris or retina patterns, fingerprints, voice, and even DNA. By capturing and storing these unique identifiers in a database, biometric systems enable the verification of an individual's identity with a high degree of accuracy. When an individual seeks access to a system or dataset, their biometric information undergoes comparison with the stored data, facilitating authentication[2].

I. Introduction

The journey of biometric identification has been marked by significant advancements in technology and its integration into various domains of society. From its nascent stages to its widespread adoption, biometrics has revolutionized the landscape of identity verification. The evolution of biometric systems has been propelled by the imperative of enhancing security measures while concurrently streamlining

[1] Student at Amity Law School, Noida

[2] National Research Council et al., Biometric Recognition: Challenges and Opportunities (2010).

authentication processes. However, the efficacy and utility of biometric identification are contingent upon the establishment of a robust legal framework to govern its usage. The legal framework serves as a bulwark against potential misuse or abuse of biometric data, safeguarding individuals' rights and privacy[3]. Through a comprehensive set of laws and regulations, the legal framework delineates the parameters within which biometric technology can operate, ensuring adherence to ethical standards and principles of fairness.

Central to the legal framework governing biometric identification are provisions aimed at protecting individuals' privacy rights and personal data. In many jurisdictions, laws such as GDPR in the European Union and the California Consumer Privacy Act (CCPA) in the United States mandate stringent measures for the collection, storage, and processing of biometric information. These regulations impose obligations on organizations to obtain explicit consent from individuals before collecting their biometric data and to implement robust security measures to prevent unauthorized access or disclosure. Moreover, the legal framework encompasses provisions concerning the transparency and accountability of entities deploying biometric systems. Organizations are often required to disclose the purpose and scope of biometric data collection, as well as the mechanisms for obtaining consent and exercising individuals' rights over their data. Additionally, accountability mechanisms, such as data protection impact assessments and regular audits, serve to ensure compliance with legal obligations and mitigate the risks associated with biometric technology.

In the realm of law enforcement and national security, the use of biometric identification introduces complex ethical and legal considerations. While biometrics offer potent tools for enhancing public safety and combating crime, their deployment must be subject to rigorous oversight and accountability mechanisms. Legal frameworks governing law enforcement biometrics often prescribe strict limitations on the retention and sharing of biometric data, as well as safeguards against unlawful profiling or discrimination. Today the legal framework surrounding biometric identification extends to issues of data retention, deletion, and access rights. Individuals are typically granted rights to access their biometric data, rectify inaccuracies, and request its deletion in accordance with applicable laws. Moreover, organizations are

[3] Anil K. Jain, Debayan Deb & Joshua J. Engelsma, *Biometrics: Trust, But Verify*, 4 IEEE Transactions on Biometrics, Behavior, and Identity Science 303 (2022).

tasked with establishing robust data retention policies to ensure the lawful and responsible handling of biometric information throughout its lifecycle.

II. Evolution of Biometric Identification Methods

The historical journey of biometric identification spans centuries, with notable milestones dating back to ancient China. European explorer Joao de Barros documented the earliest known example of fingerprinting during the 14th century, where Chinese merchants utilized ink to record children's fingerprints for identification purposes. This early instance underscores the enduring human fascination with leveraging unique biological traits for authentication and verification. In the late 19th century, Alphonse Bertillon pioneered the field of anthropometry, employing body measurements and physical characteristics to aid in criminal identification. His method, known as the Bertillonage method, gained widespread adoption by law enforcement agencies until its limitations became apparent. The Bertillonage method's fallibility prompted a shift towards fingerprinting, championed by Richard Edward Henry of Scotland Yard, marking a pivotal moment in the evolution of biometric identification techniques. Karl Pearson, an influential applied mathematician of the early 20th century, made significant contributions to biometric research through his groundbreaking work in statistical analysis and correlation. Pearson's insights laid the foundation for modern biometric methodologies, including the method of moments, the Pearson system of curves, and correlation analysis. His pioneering efforts advanced the scientific understanding of biometric characteristics and their applicability in diverse domains, from animal evolution to human identification.[4]

The 1960s and '70s witnessed the emergence of signature biometric authentication procedures, albeit with limited adoption and efficacy. However, it was not until military and security agencies delved into biometric research and development beyond fingerprinting that the field experienced renewed interest and progress. The advent of advanced biometric technologies has transformed authentication practices, offering enhanced security measures and efficiency in identity verification processes[5]

Despite the technological advancements and widespread adoption of biometric

[4] Sudeep Tanwar et al., *Ethical, Legal, and Social Implications of BiometricTechnologies*, *in* Biometric-Based Physical and Cybersecurity Systems 535 (Mohammad S. Obaidat, Issa Traore, & Isaac Woungang eds., 2019).
[5] Leonard A. Jackson, *Biometric Technology: The Future of Identity Assurance and Authentication in the Lodging Industry*, 21 International Journal of Contemporary Hospitality Management 892 (2009).

authentication, the field remains mired in controversy and ethical dilemmas. Civil liberties groups' voice concerns over privacy infringements and identity issues inherent in biometric systems, raising questions about the balance between security imperatives and individual rights. As biometric laws and regulations continue to evolve, stakeholders grapple with the complexities of safeguarding privacy while harnessing the benefits of biometric technology.

In contemporary discourse, biometric characteristics are broadly categorized into physiological and behavioural traits. Physiological biometrics, such as fingerprints, face recognition, hand geometry, and iris recognition, are inherently linked to the physical attributes of individuals and exhibit unique variations among different persons. Conversely, behavioural biometrics, encompassing traits like signature dynamics, keystroke patterns, and voice recognition, derive from the behavioural patterns and habits of individuals[6].

The emergence of cognitive biometrics represents a novel frontier in the field, bridging human perception with computer databases through brain-machine interfaces. Cognitive biometrics leverage specific brain responses to external stimuli as identifiers, offering potential applications in security and authentication systems. This innovative approach holds promise for advancing the frontier of biometric technology, paving the way for new paradigms in identity verification and access control.[7] In the contemporary landscape, the convergence of technological advancements and societal imperatives drives ongoing innovation and debate in the field of biometrics. While the proliferation of biometric authentication holds transformative potential for security and convenience, it also raises fundamental questions about privacy, consent, and ethical considerations. As researchers and developers continue to push the boundaries of biometric technology, the need for robust legal frameworks and ethical guidelines becomes increasingly imperative to ensure responsible and equitable deployment in society.

i. Early Biometric Identification Methods

Prior to the age of advanced technology, humans devised inventive methods of

[6] Andrea North-Samardzic, *Biometric Technology and Ethics: Beyond Security Applications*, 167 J Bus Ethics 433 (2020).

[7] Denise Almeida, Konstantin Shmarko & Elizabeth Lomas, *The Ethics of Facial Recognition Technologies, Surveillance, and Accountability in an Age of Artificial Intelligence: A Comparative Analysis of US, EU, and UK Regulatory Frameworks*, 2 AI Ethics 377 (2022).

identifying one another based on distinct physical traits. These early kinds of biometric identification helped to lay the groundwork for modern procedures and continue to influence current practices.

1. Fingerprints

One of the first biometric identifiers recognised by humans was fingerprints. Around 2000 BCE, the ancient Babylonians utilised fingerprints on clay tablets for business transactions. Around 700 CE, the Chinese utilised inked fingerprints as signatures on documents. Scientists such as Sir Francis Galton researched and classified fingerprint patterns in the nineteenth century, paving the way for the systematic use of fingerprints for personal identification. The evolution of fingerprints as a tool of identification is quite fascinating. Many scientists researched and contributed to the development of fingerprints as 'AN INFALLIBLE EVIDENCE'.[8] Fingerprints are still one of the most reliable and extensively used biometric identifiers today, and they are an important aspect of criminal investigations.

2. Facial Recognition

Recognising persons based on their facial traits is a natural human capacity that served as the foundation for early face recognition technologies. Portraits and sculptures were used to distinguish individuals in ancient civilizations such as Egypt and Rome. Around 700 CE, the Chinese began "*face printing*" on clay figures, imprinting the unique facial traits of labourers on payment paperwork. The practise of recognising or verifying a person's identification using their face is known as facial recognition. It records, analyses, and compares patterns based on facial information. Face identification is an important step in detecting and finding human faces in photos and movies. Based on the person's facial traits, the face capture technique converts analogue information (a face) into digital information (data or vectors).[9] The face matching procedure determines whether two

[8] Brian E. Dalrymple, *Fingerprints*, *in* the Forensic Laboratory Handbook: Procedures and Practice 117 (Ashraf Mozayani & Carla Noziglia eds., 2006).
[9] Vicki Bruce & Andy Young, *Understanding Face Recognition*, 77 British J of Psychology 305 (1986).

faces belong to the same person. While early facial identification relied on human memory and artistic depiction, modern facial recognition technology uses algorithms to analyse and compare facial traits, allowing it to be integrated into a wide range of applications such as security systems and personal devices.

3. Other Early Methods

In addition to fingerprints and facial recognition, other early forms of biometric identification included hand geometry, which used the size and shape of hands to identify individuals; voice recognition, which relied on individuals' distinct vocal characteristics; and even physical marks or tattoos on the body. These tactics, while primitive by modern standards, underlined the underlying human desire to distinguish and authenticate individuals. In essence, the early types of biometric identification represent our forefathers' intelligence and inventiveness in finding methods to verify identity. These methods paved the way for today's sophisticated biometric technologies, reminding us of the timeless need of recognising and identifying persons for practical and security reasons.

b. Biometrics Technological Advances and Innovations

The extraordinary technological improvements and imaginative innovations that have spurred the rapid evolution of biometric identification methods. These innovative solutions have changed the face of identity verification and identification, ushering in a new era of precision, security, and simplicity.

- **Iris Recognition**

Iris recognition exemplifies the intricate miracles of biometrics. It is a biometric identification system based on mathematical pattern recognition techniques applied to video pictures. In comparison to other modalities, the complex metrics of this identification method are distinctive, rapid, and stable.[10]Iris recognition generates an extremely reliable identifier by obtaining high-resolution photos of the unique patterns in the coloured area of the eye. The iris' complex network of lines, forms,

[10] Xingyu Jiang et al., *A Review of Multimodal Image Matching: Methods and Applications*, 73 Information Fusion 22 (2021).

and colours is nearly impossible to replicate, giving an unrivalled level of security. This technology has found uses ranging from securing access to sensitive facilities and secret data to providing smooth and secure authentication in daily gadgets.

- **Voice Recognition**

Using advances in signal processing and machine learning, voice recognition has revolutionised the way we engage with technology. This technique converts speech into a unique biometric signature by analysing vocal parameters such as pitch, tone, and cadence. Voice recognition offers a wide range of applications, from phone-based customer service verification to smart home gadgets that recognise and respond to unique voices.[11]

- **DNA Profiling**

The human genome, a treasure store of information that is unique to each individual, has laid the groundwork for DNA profiling. DNA profiling is the process of obtaining a specific DNA pattern, known as a profile, from a person or a sample of body tissue. Technological advancements in DNA sequencing and analysis have allowed forensic specialists and researchers to unravel an individual's genetic makeup with unprecedented precision. DNA profiling not only benefits in crime solving and relationship formation, but it also has enormous potential for personalised treatment and disease prediction.

- **Gait Analysis**

Just like our fingerprints, the way we walk has become a topic of biometric research. Gait analysis, made possible by advances in motion capture and computer vision, examines the rhythm and pattern of a person's gait. This approach is particularly appealing for security and surveillance applications in which standard biometrics may be problematic or unavailable.

c. Biometric Identification Integration across Sectors

The integration of biometric identification technologies represents a significant milestone in the evolution of various sectors, profoundly impacting law enforcement,

[11] R.V. Cox et al., *Speech and Language Processing for Next-Millennium Communications Services*, 88 Proceedings of the IEEE 1314 (2000).

healthcare, finance, access control, and border control and immigration. This transformation has been driven by the capabilities of biometric systems to provide rapid and accurate identification through unique physiological or behavioral characteristics such as fingerprints, facial features, iris patterns, and palm veins. The multifaceted applications of biometrics have ushered in a new era of security, efficiency, and convenience across different domains, while also raising ethical and regulatory considerations to ensure responsible deployment and safeguard individual privacy.[12]

In law enforcement, biometric identification has emerged as a powerful tool for enhancing public safety and expediting criminal investigations. By leveraging fingerprint and facial image databases, law enforcement agencies can swiftly identify suspects and apprehend dangerous individuals. The use of biometrics has revolutionized the traditional methods of suspect identification, replacing time-consuming and error-prone processes with streamlined workflows that yield higher accuracy and efficiency.[13] Furthermore, biometric technologies have enabled the automation of identification processes, allowing law enforcement personnel to focus their efforts on other aspects of investigations, thus accelerating the resolution of cases and improving overall outcomes.

Similarly, in the healthcare industry, biometric identification plays a crucial role in ensuring patient safety and improving the quality of care. By accurately identifying patients through their unique biometric traits, healthcare providers can mitigate the risk of medical errors, such as administering treatments to the wrong individual or accessing incorrect medical records. Biometric authentication also facilitates the seamless sharing of medical information between different healthcare institutions, enabling healthcare professionals to access critical patient data promptly and make well-informed decisions. As a result, patients receive more personalized and effective care, leading to better health outcomes and increased satisfaction with the healthcare experience.

[12] Abdul Saboor et al., *Latest Research Trends in Gait Analysis Using Wearable Sensors and Machine Learning: A Systematic Review*, 8 IEEE Access 167830 (2020).

[13] G. M. S. Ross et al., *Best Practices and Current Implementation of Emerging Smartphone-Based (Bio)Sensors – Part 1: Data Handling and Ethics*, 158 TrAC Trends in Analytical Chemistry 116863 (2023).

d. Biometric Identification Adoption and Implementation

The widespread integration of biometric identification technology has ushered in a new era of secure and efficient verification practices across multiple industries, fundamentally transforming the way individuals establish their identity in various facets of daily life. From government initiatives to private sector applications, biometrics have become increasingly ubiquitous, revolutionizing traditional methods of authentication and verification. Governments worldwide are embracing biometric technology as a cornerstone of comprehensive national identity systems aimed at creating watertight identity records for citizens. These systems leverage unique biometric identifiers such as fingerprints, iris scans, and facial recognition to enhance government service delivery, streamline administrative processes, and mitigate identity fraud. By implementing biometric identification programs, governments can improve the accuracy and reliability of citizen identification, thereby bolstering national security and facilitating efficient governance.

In the realm of border control and immigration, biometric identification has significantly altered standard procedures, particularly at airports and checkpoints.[14] Facial recognition and iris scanning technologies are now commonly employed to expedite traveler processing while simultaneously enhancing security measures and reducing wait times. By capturing and verifying biometric data, border control agencies can ensure the proper identification of individuals, thereby fortifying border security and safeguarding against potential threats to national sovereignty.

e. The Advantages and Difficulties of Biometric Identification

The use of biometric identification has various advantages, including higher security, reduced fraud, increased efficiency, and a better user experience. However, this movement raises serious concerns about data privacy, security breaches, and the potential abuse of biometric information. As biometric measures grow more incorporated into our lives, maintaining a balance between convenience and data security becomes increasingly important. The adoption and implementation of

[14] Ian Hosein, *Transforming Travel and Border Controls: Checkpoints in the Open Society*, 22 Government Information Quarterly 594 (2005).

biometric identification has changed the way people engage with governments, organisations, and technology. As this trend continues, it will be critical to maintain ethical standards, build strong regulatory frameworks, and ensure that the benefits of biometrics are realised while protecting individuals' privacy and rights.[15]

The use of biometric identification systems has provided numerous benefits, revolutionising how we establish and verify identity. The good news is that biometrics are exceedingly difficult to decipher. This is because the differences are so distinct or nuanced that replicating them requires complex tools, calculation, and distinct data. The voice, for example, contains well over 100 qualities that are unique to each individual. Similarly, fingerprints would necessitate some type of physical connection in order to be replicated. However, these advantages are accompanied by a number of complicated ethical and privacy issues that must be carefully considered.

f. Benefits of Biometric Identification Techniques

Biometric identification has emerged as a cornerstone of security and fraud prevention, offering a virtually foolproof method of verifying identity. Unlike traditional authentication techniques such as passwords or PINs, biometric markers are unique and impossible to replicate, making unauthorized access significantly more challenging. This heightened security feature has proven especially valuable in high- security organizations, financial institutions, and digital transactions involving sensitive information. By leveraging biometric technology, organizations can bolster their security measures and protect against potential threats to data integrity and confidentiality.[16]

In addition to enhanced security, biometric identification offers unparalleled convenience and efficiency in authentication processes. By eliminating the need to memorize and manage multiple passwords or access cards, biometric solutions streamline user authentication, providing a smooth and user-friendly experience. This not only reduces the frustration associated with forgotten passwords but also accelerates access to various services and resources. Whether unlocking devices or entering secure locations, biometric authentication saves time and effort, enhancing operational efficiency and productivity for both individuals and organizations.

[15] L. D. Adkins, "*Biometrics: Weighing Convenience and National Security against Your Privacy*" 13 Mich. Telecomm. & Tech. L. Rev. 541 (2006).

[16] Ali M Al-Khouri, *Digital Identity: Transforming GCC Economies*, 16 Innovation 184 (2014).

Moreover, biometric identifiers such as fingerprints, iris scans, or speech patterns ensure accurate identification and verification, even in high-stakes scenarios such as law enforcement investigations. The precision of biometric technology minimizes the occurrence of false positives and false negatives, resulting in more reliable decision-making processes and outcomes.[17] This accuracy is paramount in situations where swift and precise identification is crucial, underscoring the importance of biometric technology in enhancing security measures and supporting effective governance. However, alongside the numerous benefits of biometric identification, concerns regarding ethics and privacy loom large, necessitating careful consideration and robust safeguards. The preservation and storage of sensitive biometric data represent a significant ethical concern, demanding stringent encryption and security measures to prevent breaches that could lead to identity theft or unauthorized access. Furthermore, the collection and storage of biometric data raise fears of potential theft or hacking, exposing individuals to the risk of identity theft or financial crime. Unlike passwords or PINs, biometric data is immutable, underscoring the urgency of safeguarding this information from unauthorized access or misuse.

As biometric surveillance becomes increasingly prevalent, apprehensions regarding the potential misuse of data for mass surveillance or tracking individuals without their consent intensify. Balancing the imperative of enhanced security with the imperative of protecting individual privacy necessitates comprehensive regulations and oversight mechanisms to mitigate potential abuses of biometric technology. Moreover, the collection and use of personal biometric data raise concerns regarding informed consent and user control, highlighting the importance of transparency and user autonomy in biometric identification practices.

A biometric data breach can have far-reaching implications, compromising an individual's identity indefinitely. Unlike passwords, biometric markers cannot be altered or modified if compromised, underscoring the criticality of safeguarding sensitive information from unauthorized access. While the advantages of biometric identification systems are undeniable, addressing the ethical and privacy challenges inherent in their deployment is paramount to ensuring responsible and equitable application. Striking a delicate balance between security imperatives and privacy rights will be essential in realizing the full potential of biometric identification while

[17] A.K. Jain, A. Ross & S. Prabhakar, *An Introduction to Biometric Recognition*, 14 IEEE Transactions on Circuits and Systems for Video Technology 4 (2004).

safeguarding individuals' digital identities and preserving their fundamental rights.[18]

g. The Legal and Regulatory Environment for Biometric Identification

Usage of Biometric Data Authentication has become the new norm as it has been to solve a lot of security issues.[19] The fast spread of biometric identification technology has created an urgent need for strong legal and regulatory frameworks to protect individual rights, privacy, and data security. This study digs into the complicated environment of biometric identity law, showcasing the convoluted web of international standards, national legislation, and case studies.

- ***Concerns about Ethics and Privacy International Guidelines and Standards***

Adopted by the United Nations in 1948, the Universal Declaration of Human Rights establishes the framework for the protection of individual rights in the digital era. Whereas acknowledging the inherent dignity and equal and inalienable rights of all members of the human family is the foundation of global freedom, justice, and peace. According to Art. 12 and 19 emphasise the right to privacy and the significance of informed consent, both of which are important to biometric identification. However, applying and interpreting these ideas to developing biometric technologies presents complex hurdles.

The GDPR of the European Union is a watershed moment in data protection and privacy. It has a significant influence on biometric identification, necessitating severe safeguards for the collection, processing, and storage of biometric data. When an individual uses personal data for purposes outside than the personal sphere, such as socio-cultural or financial activities, the data protection regulation must be followed. The GDPR's data minimization, purpose limitation, and individual rights principles apply to biometrics, emphasising the necessity for explicit consent and rigorous security measures.

- **National Policies and Legislation**

Many countries have enacted legislation to protect biometric data. The Aadhaar

[18] K.A. Toh, X. Jiang & W. Y. Yau, *Exploiting Global and Local Decisions for Multimodal Biometrics Verification*, 52 IEEE 3059 (2004)

[19] T. Devi, *Biometric Data, Identification and Authentication in India – Legal Framework, Challenges and Impact*, 4 IJLMH 1001 (2021).

Act, for example, oversees India's unique identity programme, specifying standards for data security, permission, and usage constraints. Similarly, Biometric Information Privacy Acts in certain states, such as Illinois, govern the collecting and storage of biometric data in the United States. These regulations emphasise transparency, informed consent, and strict biometric data protection.[20]

Legal frameworks that are effective emphasise the responsible and transparent use of biometric data. Biometric data collection and use are frequently restricted by law. For example, the Privacy Act of Australia and the Data Protection Act of the United Kingdom both prohibit the use of biometrics for employee monitoring or surveillance. These measures are intended to prevent the exploitation of biometric data while allowing genuine applications because biometric data frequently crosses national borders, cross-border data transfer procedures are required. The "Schrems II" judgement of the European Court of Justice emphasises the need of maintaining proper data protection procedures when transferring biometric information internationally. This judgement has an influence on the global flow of biometric data, demanding complex legal systems to maintain privacy standards.

- **Legal Disputes and Court Decisions**

In April 2015, IT professionals at the United States Office of professionals Management (OPM), the agency in charge of the government's civilian workforce, found that some of its personnel files had been compromised. The 2015 hack of the US Office of Personnel Management (OPM) revealed the risks of biometric data. The breach exposed millions of fingerprints, sparking concerns about culpability and compensation for those affected. This case emphasises the importance of robust security measures and the establishment of accountability for data breaches.

When recognising women of colour, 35% of facial recognition errors occur, compared to 1% for white males. Legal issues in facial recognition have arisen due to worries about false positives, racial bias, and invasive surveillance. Cases such as the *American Civil Liberties Union (ACLU)* v. *Clearview*[21] AI highlight the ethical and legal quandaries surrounding the influence of facial recognition on privacy, public safety, and individual rights.

[20] Jeroen van den Hoven, *Privacy and the Varieties of Informational Wrongdoing*, *in* Computer Ethics (2007).
[21] *ACLU* v. *Clearview AI*, 2021 Ill. Cir. LEXIS 292.

India's Aadhaar programme, one of the world's largest biometric identification programmes, has encountered legal issues involving privacy and data protection.[22] The momentous judgement by India's Supreme Court affirmed the program's constitutionality while emphasising the significance of protecting biometric data and respecting individual privacy. The legal and regulatory framework for biometric identification is complex and multifaceted, covering international treaties, national legislation, and real-world case studies. The problem is to create frameworks that maximise the benefits of biometric technologies while protecting fundamental rights and individual autonomy. In our increasingly networked and data-driven world, striking this balance is not only a legal need, but also a moral obligation.

h. Biometric Innovation and Privacy Rights

The dynamic interplay between biometric innovation and the protection of privacy rights represents a critical junction in today's rapidly evolving technology landscape. As biometric technologies continue to advance at a remarkable pace, their widespread adoption has raised significant concerns regarding the potential implications for individual privacy and data protection. At this pivotal juncture, it is imperative to conduct a comprehensive assessment of key concerns to effectively navigate the delicate balance between promoting the development of cutting-edge biometric technology and safeguarding the fundamental rights of individuals. One of the primary considerations in this dialogue is the inherent tension between the benefits of biometric innovation and the potential risks to privacy. While biometric identification offers unparalleled accuracy and security in authentication processes, it also entails the collection and storage of sensitive biometric data, raising concerns about the potential for unauthorized access, misuse, or abuse.[23] Therefore, any discussion surrounding biometric innovation must carefully weigh the potential benefits against the potential risks to privacy and ensure that adequate safeguards are in place to protect individuals' personal information.

- **The Importance of Informed Consent and User Education**

The notion of informed consent is crucial to the ethical use of biometric

[22] Pam Dixon, *A Failure to "Do No Harm" -- India's Aadhaar Biometric ID Program and Its Inability to Protect Privacy in Relation to Measures in Europe and the U.S.*, 7 Health Technol. 539 (2017).
[23] T. Satpathy, "*The Aadhaar: 'EviL' Embodied as Law"* 7 Health Technol. 469 (2017).

technologies. Individuals must understand how their biometric information will be collected, kept, and used. To ensure that individuals provide informed and voluntary consent, consent processes should be visible, accessible, and understandable. It is critical to raise user understanding of biometric technology's capabilities, benefits, and potential concerns. Individuals are better equipped to make informed judgements about sharing their biometric data when they are educated about the ramifications. Public awareness campaigns, privacy policies, and user-friendly interfaces all help to build an informed and alert user base.

- **Policies for Biometric Data Retention and Deletion**

Biometric data retention policies should indicate how long data will be kept. Data should not be retained permanently, and retention durations should be decided in accordance with legitimate goals and regulatory constraints. Data should be erased as soon as the purpose is completed to reduce the risk of unauthorized access or misuse.[24]

Giving people the ability to seek the deletion of their biometric data strengthens their control over their personal information. This right is consistent with privacy standards and helps individuals to manage their digital footprint, especially after their relationship with the data collector ends.

- **Biometric Technology Provider Accountability and Transparency**

1. Before installing biometric systems, biometric technology suppliers should complete rigorous data protection impact assessments. These assessments detect potential threats to people' privacy and aid in the development of risk-mitigation solutions. Accountability and responsible data handling are promoted through transparent documentation of these assessments.
2. Privacy should be the default setting in biometric systems. This includes limiting data collecting to authorised individuals and prioritising data security. Users who do not want to employ biometric identification should be permitted to do so without fear of repercussions.

The delicate balance of biometric innovation and privacy rights is dependent on proactive steps that empower users, promote openness, and hold technology companies

[24] C. L. Miltgen, A. Popovič & T. Oliveira, "*Determinants of End-User Acceptance of Biometrics: Integrating the "Big 3" of Technology Acceptance with Privacy Context"* 56 DSS 103 (2013).

accountable. Society can leverage the potential of biometrics while safeguarding individual autonomy and dignity in an increasingly digital world by prioritising informed permission, enforcing reasonable data retention policies, and ensuring accountability.

The Biometric Information Privacy Act (BIPA) of Illinois was enacted in 2008 and is widely regarded as one of the most restrictive state laws governing biometric data. Private organisations must tell employees before collecting or retaining biometric data, obtain written consent, and make certain disclosures under BIPA. In addition, covered businesses must create retention plans and protocols for permanently destroying biometric data. BIPA forbids the sale of gathered biometric data, requires such data to be protected in accordance with industry standards, and provides a private right of action for technical violations. Statutory penalties range from $1,000 per infraction to $5,000 for willful or careless violations, prompting class-action lawsuits.[25]

In the Texas enacted CUBI in 2009, requiring informed permission for biometric data gathering without the requirement of written consent. Entities must notify data subjects before collecting biometric information and guarantee that it is protected in the same way as other sensitive data. Unlike BIPA, CUBI delegated sole enforcement authority to the state's attorney general, with potential restitution limited to $25,000 per violation.

In 2017, Washington followed suit, establishing legislation modelled after Texas'. In Texas, the act can only be enforced by the state's attorney general, potentially indicating a developing trend of enforcement being limited to official channels.[26] Given the popularity of biometrics in a variety of situations, including workplaces, and the serious repercussions of data breaches, other states are likely to enact restrictions. As biometric technology advances, more jurisdictions may choose to build complete legal frameworks to protect the privacy and security of biometric data. This comparative analysis highlights the disparities in state approaches to controlling biometric data, with Illinois' BIPA standing out as a particularly stringent framework, Texas' CUBI presenting a separate enforcement methodology, and Washington's legislation agreeing with Texas' approach. As the use of biometric data grows, the legal environment may evolve to ensure proper management and protection of this sensitive information.

[25] U. Uludag et al., *Biometric Cryptosystems: Issues and Challenges*, 92 Proceedings of the IEEE 948 (2004).

[26] *Evidence on Enforcement of Federal Environmental Statutes*, 82 J. Crim. L. & Criminology 1054 (1991).

Today biometric technology has become a transformative force in the modern technological landscape, fundamentally reshaping the way individuals establish and verify their identities. This innovation relies on capturing and analyzing unique physiological traits such as fingerprints, iris patterns, and facial features to ensure precise and reliable identification. In the global push towards digitization, biometric systems stand out for their ability to address the limitations of traditional identification methods, offering enhanced security, accuracy, and convenience. India's Aadhaar programme is a prominent example of how biometric technology is being leveraged to create a robust framework for identity verification, with significant implications for governance, service delivery, and societal inclusion.

REFERENCES

- Ahuja, I. & Kapadia, S. (2023). Understanding the DPDP Act 2023. *Bar & Bench*. barandbench.com (accessed June 30, 2025).
- Alpha Partners. (2022). India's Privacy Reform Update. *Mondaq*. mondaq.com (retrieved June 30, 2025).
- Amnesty International. (n.d.). Summary on the UDHR. amnesty.org (viewed June 30, 2025).
- Banerjee, S. & Bharuka, A. (n.d.). Transitioning to New Data Framework. *SCC Blog*. scconline.com (visited June 30, 2025).
- Bhandari, V. et al. (n.d.). Revisiting the Puttaswamy Verdict. *IndraStra*. indrastra.com (consulted June 30, 2025).
- Burman, A. (n.d.). Key Insights on India's Data Law. *Carnegie India*. carnegieindia.org (accessed June 30, 2025).
- Chakraborty, S. & Chatterjee, H. (n.d.). Hospitality Sector & DPDP. *SCC Online Blog*. scconline.com (retrieved June 30, 2025).
- Chopra, R. & Ramani, M.M. (2021). Privacy & OTT Compliance. *Mondaq*. mondaq.com (viewed June 30, 2025).
- Cortez, E.K. (n.d.). Comparative Review: Privacy Regulations Worldwide.
- Data Protection Helpdesk. (2024). India's Regulatory Landscape. Intellectual-property-helpdesk.ec.europa.eu (accessed June 30, 2025).
- Didomi. (n.d.). Understanding Singapore's PDPA. blog.didomi.io (visited June 30, 2025).
- DLA Piper. (n.d.). Country Comparison Tool: Data Laws. dlapiperdataprotection.com (consulted June 30, 2025).
- Doyle, C. (2012). ECPA Summary. *HSDL*. hsdl.org (accessed June 30, 2025).
- East Asia Forum. (2022). Balancing Privacy & Progress in India. eastasiaforum.org (retrieved June 30, 2025).