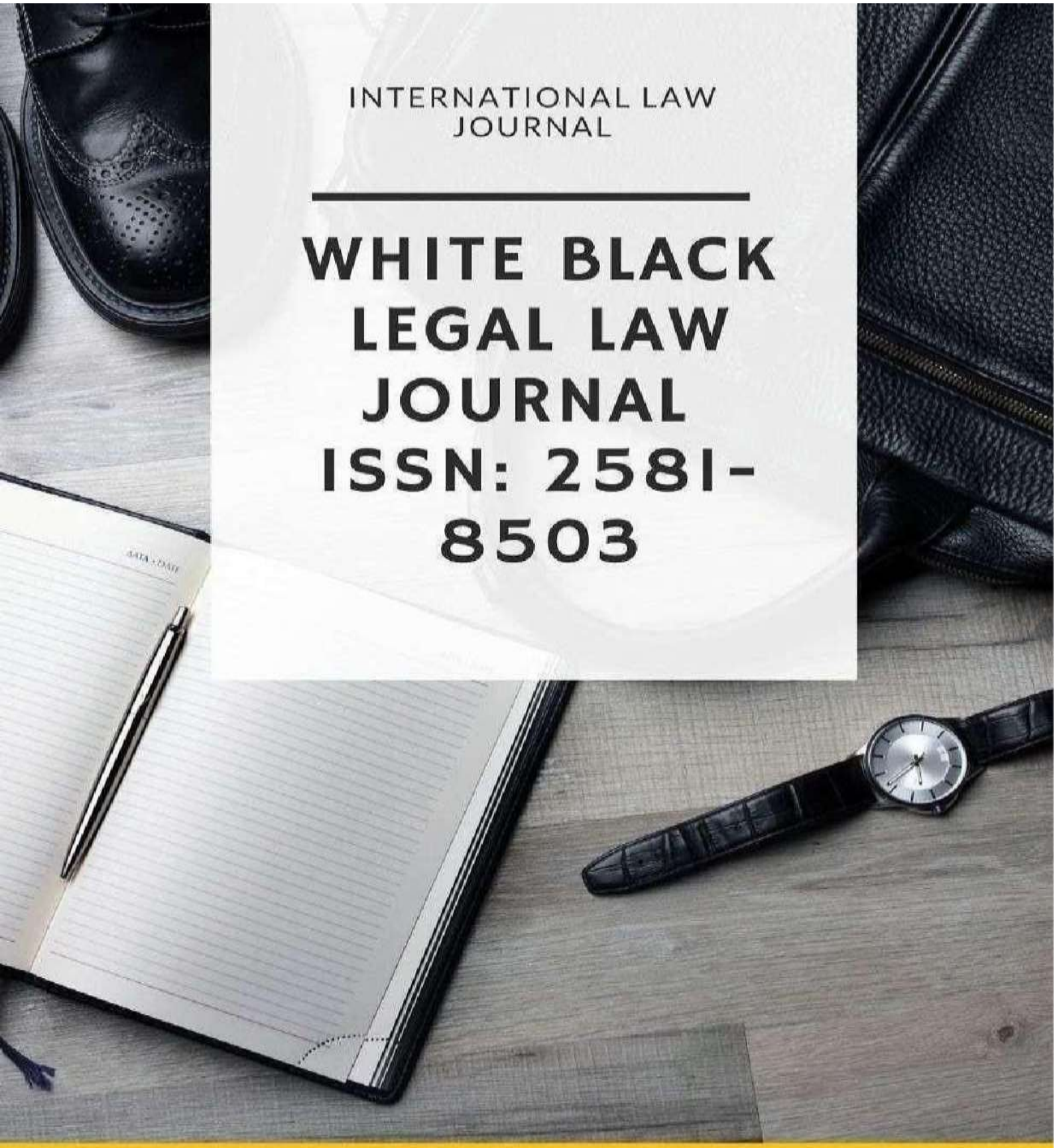

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

BIOMETRIC DATA AND TRADE SECRETS CAN CONFIDENTIALITY PROTECT WHAT IS INHERENTLY PUBLIC?

AUTHORED BY - SONALI SINGH & ADITI AISHWARYAM

ABSTRACT

Biometric data like fingerprints, face traits, and voice patterns that contain an underlying paradox: they are unique and available to the complete community. Proper trade secrets are valuable because they are secret. Biometric identifiers, unlike trade secrets proper, are not capable of absolute concealment from ordinary exposure. This brings up an essential question: Is it justified to preserve something that is de facto public by secrecy regimes? This research investigates the relationship between legal theories of trade secret protection and the visibility of biometric features. It considers if human traits that are visible can become hidden knowledge that can be protected by contract, technology means, and legal systems. A comparison of data protection regimes, privacy laws, and intellectual property laws shows the fine line between individual freedom and commercial interests. Ultimately the research speaks to a reassessment of confidentiality in the age of biometric commodification when the border between corporate data and public identification is becoming blurred.

KEYWORDS
Biometric Data, Trade Secrets, Confidentiality, Privacy Law and Public Identity.

INTRODUCTION

Biometric data, such as fingerprints, facial geometry, iris scans, and voice patterns, has become a cornerstone of current identification systems. It is attractive because of its individuality and durability. This also makes it dependable yet not easy to imitate. But these same attributes also reveal a paradox: biometric identifiers are essentially public. Biometric features are obvious in daily interactions, but passwords or trade secrets get their worth from obscurity. You can take a picture of a face, record a voice, and watch a stride. This poses a fundamental legal question: can secrecy shield what is essentially in the public domain?

Trade secret law traditionally has protected knowledge that is economically valuable because

it is secret. The theory assumes concealment. Protection is based on reasonable efforts to maintain secrets. Biometric data disproves that assumption. The basic characteristics themselves are not secret, but the algorithms, databases, and processing techniques used to store and match biometric identifiers can be. This tension challenges the classification of biometric data as a trade secret, as the observable nature of biometric data affects the secrecy factor.

Confidentiality frameworks include contractual duties, non-disclosure agreements, and technical measures, which are increasingly being called upon to protect biometric information. Employers, corporations, and governments say that, even if the physical characteristics are public, the digital representations, templates, and analytical models are proprietary. This contrast between the "observable" and "processed" form of biometric data is at the heart of ongoing issues in intellectual property and privacy law. But whether secrecy may safeguard data obtained from otherwise public aspects, and if so under what terms, is an issue courts and legislators struggle with.

The stakes are high. In addition to being a form of verification, biometric data is a commodity that sustains surveillance economies, a resource for artificial intelligence, and a potential source of privacy abuses. Secrecy may commodify identity itself by converting public features into protected property. But denying protection can leave people and organizations vulnerable to fraud, abuse, and exploitation. Social trust, commercial interests, and individual liberty are difficult to balance.

REVIEW OF LITERATURE

Fingerprints, faces, and other biometric data make it easier to prove who you are, but they also raise privacy issues under regulations like GDPR. The literature emphasizes that it cannot be undone and can be misused. A trade secret is a secret that is kept secret for business purposes. The TRIPS Agreement and Indian law both place importance on economic value. Both areas have to balance rights and innovative ideas.

HYPOTHESIS

How can you safeguard facial features and fingerprints as trade secrets when they're out there for the world to see?

OBJECTIVE OF THE RESEARCH

1. Investigate the contradiction of genetic information as public and private.
2. Talk about trade secret theory and how it applies to biometric identifiers and stress, the importance of privacy.
3. Comparative study on rules of preserving and keeping private personal data in India, the EU, the US, and China.
4. Reflect on the significance of contractual and technological protections in the transition from visible to protectable.
5. Develop normative approaches for the protection of privacy and economic interests and the maintenance of community trust in the commercial use of biometric identification.

METHODOLOGY

This study uses a doctrinal and comparative legal research method. First, it critically evaluates the statutory provisions, judicial precedents, and scholarly commentary on trade secret legislation and the protection of biometric data. Second, it examines frameworks among jurisdictions, India, the United States, the European Union, and China, to uncover convergences and divergences in the confidentiality treatment of biometric identifiers. Third, it assesses the contractual and technological protections in place to convert observable qualities into protectable information. Finally, normative analysis is applied to provide balanced alternatives that reconcile privacy rights, financial interests, and public confidence in the commodification of biometric identification.

DEFINING BIOMETRIC IDENTIFIERS: FROM PHYSIOLOGY TO DIGITAL TEMPLATES

1. The Concept of Biometric Identifiers

Biometric identifiers are measurable biological and behavioral traits that can be utilized for the identification or verification of an individual. Unlike passwords or tokens, they are part of the human body or behavior, such as fingerprints, iris patterns, face geometry, voice, or stride. Their uniqueness and permanence make them desirable for verification but also lead to problems of whether anything essentially public, such as a face, can ever be really confidential.

2. **Physiological Biometrics: The Body as Data**

   Physiological biometrics is based on the physical characteristics of the human body. These include fingerprints, retina scans, and DNA profiles. These characteristics are biologically fixed and largely not changeable. The paradox is that they are visible: you can see the fingerprint or the face, yet the digital encoding of these qualities turns them into proprietary data. This raises the question of whether confidentiality can protect what is naturally accessible.

3. **Behavioral Biometrics: Patterns of Action**

   Behavioral biometrics is about what people do, not what they seem like. Examples include typing rhythm or voice modulations or walking away. Those identities are not fixed and can change with age, health, or environment. But once they are captured and digitized, they become ordered data sets. Digitization creates a grey area between public action and private information, where the act in its raw form is public, but the analytical framework is private.

4. **The Transition from Traits to Templates**

   The essential transition takes place when biometric features are transformed into digital templates. For example, a fingerprint image is transformed into a mathematical representation of a set of unique points or vectors. The templates are not meant to be read by humans but are secure identifiers in databases. So, secrecy is not in the raw feature itself, but in the coded representation, which is considered exclusive information.

5. **Uniqueness and Universality: The Legal Dilemma**

   Biometric identifiers are universal (everyone has them) and unique (none are the same). This duality confuses their legal position. Their universality suggests they are public in nature, yet their distinctiveness suggests they can be proprietary. Trade secret law is based on confidentiality, while biometric features are visible to the public. The question is whether digitizing these qualities adds a new layer of secret that can be protected.

6. **Confidentiality in Biometric Systems**

   A biometric template is protected using contracts, rules, and encryption. For example, they may have their employees sign agreements not to divulge fingerprint information

used in access systems. But this is simply about the data that was analyzed, not about the physical feature itself. It is worth noting that the law cannot hide a face. But it can hide how a machine sees a face.

7. Comparative Legal Perspectives

Different places employ biometric identification in different ways. In the EU, biometric data is a particular category of data under the GDPR and requires explicit agreement to process. For example, in the US, Illinois (with BIPA) and other US states have strict duties for organizations working with fingerprint data. Biometric forms are private and sensitive information in the Aadhaar system in India. The protection is more for the digital template than the raw feature.

8. Case Law and Judicial Treatment

Courts have discussed whether biometric information can be kept secret. BIPA lawsuits have also led to fines against U.S. firms for failing to keep biometric files secure. In cases relating to Aadhaar, Indian justices have emphasized the need to protect biometric records. Generally, courts establish a distinction between features exposed to the public and digital storage that is private. The prize is the completed form, and attention is directed to it.

9. Technological Mediation: From Public to Proprietary

Technology is one of the major factors in the commodification of public qualities into private assets. Algorithms can pull fine features from fingerprints, vectors from facial scans, or frequency patterns from voice recordings. These results are not visible to you directly and require advanced tools to interpret what they signify. In other words, privacy protects the technology that makes the characteristic possible, like the template, the program, and the database, but not the trait. This is what separates items that are public from those that are private.

10. Reconciling Public Traits with Confidentiality

The first step to defining biometric IDs is to resolve the dichotomy of public visibility and private encoding. Physiological and behavioral features are fundamentally public, but their digital templates are proprietary architectures. Confidentiality may not hide the human face or fingerprint itself, but it can hide the coded representation that allows

secure authentication. The legal system must therefore calibrate its approach: to protect the digital transformation, not the raw feature, and thereby reconcile trade secret law with the realities of biometric data.

TRADE SECRET LAW AND THE REQUIREMENT OF SECRECY

The trade secret law is built on the assumption that there is a form of knowledge that can draw economic value from being kept secret. Patents and copyrights, on the other hand, must be made public, but trade secrets rely on secrecy. Under the Uniform Trade Secrets Act (UTSA) in the United States and Article 39 of the TRIPS Agreement, information must not be "generally known" and is subject to "reasonable efforts" to keep it confidential. Both of these statutes emphasize the necessity for confidentiality. The courts have recognized that even while the individual components of information might be available to the general public, a unique combination or application of those components may nevertheless be a trade secret. This does not mean that the information has to be fully invisible. Using an example, if you write a recipe using common items but do not reveal the exact proportions or technique of preparation, you could protect the secret. This indicates that confidentiality is contextual; that is, it requires that knowledge not be readily available to competitors through reputable channels.

There are actual duties for the owner of the trade secret due to the need for secrecy. Businesses need to have safety measures in place such as non-disclosure agreements, limited access, encryption, and training for staff in order to demonstrate that they are taking acceptable efforts. These rights are generally subject to judicial scrutiny, and failure to enforce may undermine claims of protection. In the United States and in India, people have learned from cases like "Coca-Cola Company versus Koke Company of America"[1] and "Zee Telefilms Ltd. versus Sundial Communications Pvt. Ltd."[2] that once knowledge gets into the public domain, it cannot be taken back as a trade secret. Trade secrets are for eternity; patents pay you for disclosure with exclusive use. Trade secrets are different from other types of intellectual property rights because they can be stolen. The trade secret rules are excellent for business and lawful, since they safeguard privacy. That means private data is valuable as long as it is extremely carefully maintained safe.

[1] Coca-Cola Co v Koke Co of America 254 US 143 (1920)
[2] Zee Telefilms Ltd v Sundial Communications Pvt Ltd [2003] (5) BOMCR 404

BIOMETRIC DATA AS A TRADE SECRET: CONCEPTUAL CHALLENGES

1. The Paradox of Public Traits and Secrecy

When it comes to biometric data, trade secret law offers a basic dilemma. By their nature, biometric data such as faces, fingerprints, and voices are public, but trade secrets require that the information be private and not publicly known. Anybody can see your face or hear your voice in everyday exchanges. Such visibility undermines the entire basis of concealment. The conceptual problem is separating the raw feature, which is public, from its digital encoding, which might be proprietary. This riddle has courts and scholars wrestling: Is something that everybody can see made into a trade secret by technology intermediation? This contradiction raises questions about whether trade secret law is the right framework to safeguard biometric data or if privacy and data protection laws are more suitable.

2. Defining the Subject Matter of Protection

Trade secret law demands you be clear about what it is you are protecting. Is it the raw physiological attribute or the image collected or the processed digital template with biometric data? Each stage has its own set of problems. The raw trait is public, the image collected may be confidential, and the template processed is proprietary. But courts need to consider whether the trade secret applies only to the template or to the full chain of biometric data. This discrepancy in terminology complicates enforcement. But if only the template is protected, then the raw trait itself may not be misappropriated if viewed without permission. Alternatively, if the trait itself is private, the law risks overreaching by trying to conceal fundamentally public features behind the veil of confidentiality.[3]

3. The Requirement of Secrecy in Biometric Contexts

The law of trade secrets is based on secrecy, and biometric data creates problems for this. Biometric features are not like a chemical formula or customer list that may be hidden from public view. Every time someone walks in a public area, their face or gait is revealed. It follows that the need for secrecy must be reconsidered. Both courts and

[3] EVOLVING LANDSCAPE OF BIOMETRIC DATA PROTECTION LAWS IN INDIA – Prime Legal Law Firm Blogs

legislatures have focused on the confidentiality of the digital template, rather than the trait itself. For example, a fingerprint scan that is saved in a database could be secured if the corporation takes reasonable steps to secure it. But it causes a conceptual split: the trait is overtly displayed, but its encoding is secret. This gap brings into question whether the trade secret law is protecting the biometric identity itself or simply the technological technique that encodes it.

4. Reasonable Efforts to Maintain Secrecy

The law of trade secrets demands that the holder take reasonable steps to keep them secret. In the biometric context, this translates into encryption, access controls, and confidentiality agreements. But the efficacy of these interventions is not beyond doubt. Biometric features can be seen independently or copied even with tight precautions. For example, a person's speech can be captured without their agreement, and facial recognition systems can be taught using publicly available images." Therefore, reasonable attempts can protect the template, but they cannot prevent the trait itself from being exposed. This limits the basis of trade secret legislation, which rests on the possibility of confidentiality through vigilance. The premise that biometric data is inherently viewable and replicable is challenged.

5. The Problem of Independent Discovery

If a competitor discovers the information on his own, he is free to utilize it because it is protected under trade secret law. When fingerprints are used, an independent finding must be made. No one needs to look into a hidden database to log someone's statements or see their face. That violates privacy rules designed to protect trade secrets. Biometric features are straightforward to demonstrate, as opposed to a secret code that requires effort to decode. It is not entirely protected, because a firm can only protect the unique digital format it created, not the feature itself. The catch is that competitors could defeat the rule by obtaining their own samples of the same feature, making trade secret protection of biometric data less useful.

6. The Issue of Ownership and Control

Under trade secret law, however, the person in possession of or with access to the secret is considered to own or control the information. This assumption does not hold in the case of a fingerprint. "Biometric traits belong to the people, not to companies."

Companies that collect and hold biometric data are custodians of that data, not owners. This poses legal and moral questions: Can a company claim data about persons as a trade secret? If so, does it infringe the right to privacy and personal liberty? Trade secret laws intended to protect company secrets, not people's names. The ownership conundrum makes it hard to implement trade secret law in this context. In other words, judges are faced with balancing the right of individuals to manage their biological features versus the necessity of companies to secure data.

7. Comparative Legal Frameworks and Divergence

Governments exploit biometric data in a variety of ways, raising philosophical difficulties. Under EU legislation, biometric data is deemed to be "special category data" under the General Data Protection Regulation (GDPR) and requires specific permission to process. There are also strict limitations under state laws for organizations that process biometric data, such as the Illinois Biometric Information Privacy Act (BIPA) in the U.S. Under India's Aadhaar system, biometric data is sensitive and protected. These rules are about consent and privacy, not about protecting trade secrets. Such a discrepancy may be evidence that trade secret legislation is not the right approach to biometric data. But data security regimes are safer. The challenge is how to get the various ways to work in harmony and what role, if any, trade secret rules still play.

8. Case Law and Judicial Treatment

Protecting the privacy of genetic information has been particularly problematic, according to court decisions. U.S. companies are required by law to safeguard biometric data. Courts do this mostly to preserve privacy, not proprietary information. Indian justices in the Aadhaar issue have stressed the need to protect privacy in biometric databases. In most cases, genetic information is not protected as a trade secret. This deficiency points to the court's lack of concern for protecting trade secrets in a largely public environment. The courts protect privacy, but it's the digital formula or code, not the feature itself. The court's finding points to the core problem: biometric data doesn't fit neatly into the traditional trade secret legislation model.

9. Technological Mediation and Proprietary Value

Turning biometric features into proprietary assets is heavily dependent on technology.

Algorithms pull minutiae from fingerprints, vectors from facial scans, or frequency patterns from voice recordings. These outputs are not directly observed and require sophisticated systems to understand. Confidentiality, then, protects the technological mediation (the template, the algorithm, and the database), not the raw feature. This mediation is creating unique value, enabling corporations to assert trade secret protection on their systems. This, however, moves the attention from the biometric data itself to the technology that processes it. The basic problem is whether trade secret legislation protects biometric identifiers or only proprietary techniques of encoding such identities. This distinction is important to define the scope of protection.[4]

10. Reconciling Trade Secret Law with Biometric Realities

The last difficulty is to have trade secret rules stay up with the way fingerprint data works. Genetic knowledge is always in the public domain; trade secrets are to be kept hidden. The approach may be to just protect digital templates and technical processes and not basic features in trade secret law. Otherwise, privacy and data security policies may be a better method to keep you safe. The difficulty with this idea is that trade secret law was not developed to safeguard personal information; it was developed to protect corporate secrets. But applying it to genetic data could distort its meaning and harm people's rights. You need to understand the boundaries of trade secret law and how to blend it with the privacy laws that protect company interests as well as people's right to privacy to strike a balance.

CONFIDENTIALITY AGREEMENTS AND THEIR LIMITS IN PROTECTING BIOMETRIC INFORMATION

"Non-disclosure agreements are often used to protect private information. But the uniqueness of biometric markers makes it difficult to keep biometric information safe. Trade secrets (e.g., processes, customer lists) are inherently private. Biometric features such as fingerprints, faces, voices, and irises are public and publicly observable in nature. This means that the raw trait cannot be disguised by a privacy curtain. The agreements protect the digital format, or template, of these qualities that the companies have and employ to show who they are. Non-disclosure agreements (NDAs) and contract requirements may prevent employees, contractors, or

[4] Biometric Data Protection: Comparative Jurisprudence Across Multiple Legal Systems - Bhatt & Joshi Associates

business partners from sharing biometric templates with others. However, courts typically treat these types of agreements as evidence of "reasonable efforts" under trade secret protection statutes. But the independent discovery and replication example highlights the weakness of secrecy agreements. And a face or voice can be seen or heard by everyone without invading privacy. Competitors may also produce their own biometric samples without theft. And that's made considerably tougher by ownership and control issues. Biometric information belongs to people, not companies; thus, companies are more like caretakers than owners. There are moral and legal problems concerning whether companies should possess personal identities. In nations such as the EU (GDPR Article 9), Illinois [Biometric Information Privacy Act (BIPA)], and India (Aadhaar Act, 2016), privacy and authorization trump trade secret protection. It suggests that confidentiality agreements alone do not provide full protection. Biometric data issues are not only about the privacy of agreements but are part of the fundamental rights of persons to privacy, as some of the court cases have established, such as "Justice K.S. Puttaswamy v. Union of India"[5] and "Clayton Zellmer v. Meta Platforms Inc."[6]. Confidentiality agreements are needed to show you have done your research and prevent biometric templates from falling into the wrong hands, but they cannot change the reality that biometric features are naturally public; they cannot replace legal private rights. A combination of legal protections, strong privacy laws, technology like encryption, and respect for people's right to choose their own personal identities will make biometric data safer in the future.

COMPARATIVE LEGAL FRAMEWORKS: INDIA, EU, AND UNITED STATES APPROACHES

India, the EU and the United States have quite diverse ways of regulating biometric data. India has constitutional privacy and statutory protections such as the Aadhaar and Digital Personal Data Protection Act, while the EU has "special category data" treatment of biometrics under GDPR with strict consent requirements and the US is stuck with patchwork state regulations such as Illinois' BIPA rather than a federal one.

1. **India – Constitutional and Statutory Foundations**[7]
    - **Right to Privacy:** The Supreme Court in Justice K.S. Puttaswamy v. Union of India (2017) recognized privacy as a fundamental right, forming the constitutional basis

[5] Justice K.S. Puttaswamy (Retd) v Union of India (2017) 10 SCC 1 (SC)
[6] Clayton Zellmer v Meta Platforms Inc 104 F.4th 1117 (9th Cir 2024)
[7] Biometric Data Privacy Laws in India: Powerful Safeguards 2026

for biometric regulation.

- **Aadhaar Act, 2016:** Governs India's national biometric identity system. Section 29 prohibits sharing biometric data except for authorized purposes.
- **SPDI Rules under IT Act, 2000:** Classified biometric data as "sensitive personal data," requiring consent for collection and disclosure.
- **Digital Personal Data Protection Act, 2023 (DPDPA):** Introduces penalties up to ₹500 crore for breaches, mandates, purpose limitation, and requires explicit consent for processing biometric data.
- **Key Challenge:** Balancing efficiency in governance (e.g., Aadhaar authentication) with risks of surveillance, exclusion, and misuse.

2. **European Union – GDPR Framework**[8]
   - **Special Category Data:** Article 9 of GDPR classifies biometric data used for identification as "special category," requiring explicit consent or a lawful basis (e.g., public interest, employment law).
   - **Data Subject Rights:** Individuals have rights to access, rectify, erase, and restrict processing of biometric data.
   - **Enforcement:** Supervisory authorities can impose fines up to €20 million or 4% of global turnover.
   - **Case Example:** The EU has scrutinized facial recognition deployments in public spaces, emphasizing proportionality and necessity.
   - **Key Strength:** Uniformity across member states ensures consistent protection, unlike fragmented US law.

3. **United States – Fragmented State-Level Regulation**[9]
   - **No Federal Law:** The US lacks a comprehensive federal biometric privacy statute.
   - **Illinois Biometric Information Privacy Act (BIPA):** The most influential state law, requiring informed consent, retention schedules, and prohibiting profit from biometric data. Provides a private right of action.
   - **Other States:** Texas and Washington have biometric laws, but enforcement is weaker. California's CCPA includes biometric data under "personal information."

[8] Biometric Data Protection: Comparative Jurisprudence Across Multiple Legal Systems - Bhatt & Joshi Associates
[9] Ibid

- **Case Law:** *Rosenbach v. Six Flags* (2019) confirmed that mere violation of BIPA's consent requirement is actionable, even without showing harm.
- **Key Weakness:** Patchwork regulation leads to inconsistent protection; companies often face litigation risks in Illinois but not elsewhere.

4. Comparison Table

ASPECT	INDIA	EU	UNITED STATES
Legal Basis	Constitutional privacy + Aadhaar + DPDPA	GDPR (Art. 9)	State laws (BIPA, Texas, Washington)
Consent Requirement	Explicit under DPDPA	Explicit under GDPR	Varies by state (strong in Illinois)
Scope	National ID + private sector	Broad, across all sectors	Fragmented, state-specific
Enforcement	Penalties up to ₹500 crore	Fines up to €20M or 4% turnover	Private lawsuits (Illinois), limited elsewhere
Strengths	Strong constitutional foundation	Uniform, comprehensive	Strong litigation rights under BIPA
Weaknesses	Risk of surveillance/exclusion	Complex compliance burden	Fragmented, inconsistent protection

5. Key Takeaways

- **India**: Strong constitutional backing, but Aadhaar controversies show risks of overreach.
- **EU**: Most comprehensive and uniform framework, emphasizing consent and proportionality.
- **US**: Powerful litigation tool in Illinois, but overall fragmented and inconsistent.

POLICY CONSIDERATIONS: BALANCING PRIVACY, INNOVATION, AND PUBLIC ACCESS

It is one of the hardest things for politicians to get the right blend of privacy, innovation, and public access today. Privacy is the right of people to control what happens with their personal information, such as health data, financial information, or activities on the internet. Individuals

may not want to provide information that can be utilized for social good or lose trust in organizations if they don't feel safe to do so. Innovation depends on the capacity to acquire knowledge. A lot has been achieved in artificial intelligence, healthcare, and education by examining very huge volumes of data. "If privacy rules are too strict, it can slow down study and make it harder to find new things." Access to knowledge and technology are very crucial to justice for the same reason, because they provide people, students, and smaller groups access to materials that would otherwise be locked away. But free access can mean private data goes public or a corporation is less eager to attempt new things if they don't want to lose their competitive edge.

The trick is to set rules that balance these three values, rather than one trumping the other two. Governments, organizations, and companies need to design institutions that protect privacy but also allow for responsible innovation and equitable public access. This balance can be achieved, for example, through de-identification of data, a request for permission prior to data sharing, and different levels of access. For example, researchers may only be permitted to utilize health data for research if personal information has been anonymized. This will safeguard privacy and allow new ideas to grow. Likewise, citizens can openly view government information without disclosing private information. It's about respecting people's right to privacy. Creative ideas that lead to advancement and transparency for everyone to make sure that everything is fair. They establish a future-proof safety culture in which trust, creativity, and mutual benefits can flourish.

CONCLUSION

Biometric data is an odd intersection of privacy, corporate secrets, and public identification. Fingerprints, face shape, and speech patterns are public and can be found in nature, but it is their digital representation as templates and algorithms that give them proprietary value. Unlike formulas or client lists, biometric features cannot be kept a secret. Trade secret law, which is fundamentally based on secrecy, has difficulty dealing with these realities. As a consequence, courts and legislatures in India, the EU, and the US have generally preferred privacy and data protection rules over trade secret regimes, with more focus on consent, proportionality, and individual rights. Confidentiality agreements and technical methods such as encryption can protect digital templates. But this does not affect the public nature of the raw material. Comparative research shows that a unified GDPR framework in the EU, fragmented state laws

in the US, and constitutional foundations in India aim to balance privacy, innovation, and commercial interests differently. In the end, safeguarding biometric data requires a hybrid approach: private technology processes that must be safeguarded under trade secret laws and individual privacy through strong regulatory regimes. Such dual recognition reconciles economic requirements with fundamental rights, underlining that confidentiality cannot alone safeguard what is fundamentally public but that a combination of legal and technical measures might sustain confidence in the age of biometric commodification.

REFERENCES

- EVOLVING LANDSCAPE OF BIOMETRIC DATA PROTECTION LAWS IN INDIA – Prime Legal Law Firm Blogs
- Biometric Data Protection: Comparative Jurisprudence Across Multiple Legal Systems - Bhatt & Joshi Associates
- Biometric Data Privacy Laws in India: Powerful Safeguards 2026

CASE LAWS

- Coca-Cola Co v Koke Co of America 254 US 143 (1920)
- Zee Telefilms Ltd v Sundial Communications Pvt Ltd [2003] (5) BOMCR 404
- Justice K.S. Puttaswamy (Retd) v Union of India (2017) 10 SCC 1 (SC)
- Clayton Zellmer v Meta Platforms Inc 104 F.4th 1117 (9th Cir 2024)