ISSN 3139-8839 (Online)

Biometric Data Ownership in AI Training: Analysing the Case for a Sui Generis Right in India

By *Shreya Das*

VOLUME I | ISSUE II | ARTICLE III

APRIL 2026

The Legalis IP Quarterly

ABSTRACT

The Indian scholarship has yet to confront a foundational legal paradox arising from the commercialisation of the biometric data as training inputs for an artificial intelligence system. India's Digital Personal Data Protection Act, 2023, classifies biometric data- fingerprints, facial geometry, voiceprints and emotional response markers as personal data and the framework for the same is built entirely on the logic of privacy and hence imposes content-based obligations on fiduciaries processing it. However, the current framework offers no answer to an equally pressing question: who owns biometric data against commercial extraction?

This paper examines the existing Indian intellectual property law and its capacity to treat biometric data as protectable subject matter. This paper aims to address three doctrinal possibilities: whether section 13 of the Copyright Act, 1957, can include the biometric data under the originality threshold, given that it is generated by a biological process rather than creative authorship; secondly, where a compilation or dataset of biometric information can qualify for database protection as an instrument lacking prominently in Indian law despite its recognition in the European union's database directive and lastly whether Indian judicial reasoning in ICC development v. Arvee enterprises and the Shivaji Rao Gaikwad line can extend the personality rights to confer a proprietary interest in one's biometric identity.

This paper further argues for the inadequacy of the frameworks, be they individual or collective, in addressing the structural legal gap, and analyses the assumption of IP law that protectable subject matter is produced rather than inhabited. The central theme of this paper is based on a comparative analysis of the Illinois Biometric Information Privacy Act and the EU AI Act's high-risk data obligations while proposing a sui generis protection model that will

serve in bridging the DPDP Act consent mechanisms with a transferrable economic right in biometric data, concluding with a doctrinal path towards accommodating the recognition of self as a source of intellectual property and not merely a subject matter of privacy.

[KEYWORDS: BIOMETRIC DATA, DPDP ACT, TRAINING DATA, SUI GENERIS PROTECTION, IP OWNERSHIP]

I. INTRODUCTION: THE PARADOX AT THE INTERSECTION OF BODY AND LAW

From the earliest debates on questions of organ commodification to reproductive rights, the human body has always been the site of legal contestation. Be it slavery or bodily autonomy, law has repeatedly been forced to decide whether the self is a subject of rights or a source of them. Biometrics in the age of AI has introduced a new and structurally distinct question: whether a person can control information about their body, including owning what they produce as an economic resource.

India's DIGITAL PERSONAL DATA PROTECTION ACT, 2023 (DPDP Act), is built on the logic of the said question, where individuals authorise or withhold the processing of their personal data by data fiduciaries through a consent-based architecture.[1] Biometric data includes fingerprints, iris scans, facial geometry and voiceprints, which require explicit consent and heightened regulatory scrutiny under Draft of Rules: Digital Personal Data Protection Rules, 2025.[2] This is treated as a particularly sensitive category; hence, a sophisticated instrument of privacy that tells us when biometric data may be processed but says nothing about who owns the economic value generated by such processing.

When this gap is seen through the lens of AI training, where a tech company ingests millions of facial images and harvests audio samples to train a facial/emotion detection system, it doesn't merely process data but extracts value from the unique individual biological characteristics and converts them into a commercial asset worth billions of dollars.[3] The current framework provides neither compensation nor attribution to the individual whose face was used to train the model, and on the other hand, the DPDP Act offers only the right to withdraw consent prospectively but offers no claim to the economic surpluses generated by the prior use of one's biometric identity.

---

[1] Digital Personal Data Protection Act, No. 22 of 2023, GAZETTE OF INDIA, pt. II sec. 1 (Aug. 11, 2023), § 1, egazette.gov.in.

[2] Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), GAZETTE OF INDIA, pt. II sec. 3(i) (Nov. 13, 2025), r. 7, https://www.dpdpa.com/dpdparules/rule7.html (last visited June 11, 2026)

[3] *Facial Recognition Market Worth $13.4 Billion by 2028, Growing at a CAGR of 16.3%: Report by MarketsandMarkets™*, Globe Newswire (Apr. 3, 2024), https://www.globenewswire.com/news-release/2024/04/03/2857078/0/en/facial-recognition-market-worth-13-4-billion-by-2028-growing-at-a-cagr-of-16-3-report-by-marketsandmarkets.html (reporting that the global facial-recognition market is projected to grow from USD 6.3 billion in 2023 to USD 13.4 billion by 2028).

This paper places the distinction between inhabited and invented at the forefront as its strongest and most original contribution, analysing the precise structural failure of existing IP frameworks. Intellectual property law is built on the foundation that a protectable subject matter is produced through an act of human creation or invention, such as authorship for copyright, invention for patent, etc. Biometric data, however, is not produced by the person but is inhabited and expressed in a measurable form. A face can't be authored, nor a fingerprint or voiceprint can be invented or compiled, yet each of these, once digitised and incorporated into an AI training pipeline, becomes a piece of valuable intellectual infrastructure.

This paper proceeds as follows: Part II reviews and analyses the literature thematically across data ownership theory, IP law's response to biometric systems, and Indian doctrinal writing on personality rights and data governance, establishing the need to address the existing legal gap that this paper aims to fill. Following up with an analysis of the three existing doctrinal candidates: copyright, database protection and personality rights. Further, it builds the affirmative argument for a hybrid sui generis model, distinguishing it from data ownership and commodification approaches in existing policy discourse, and articulating its constitutional and statutory doctrinal basis, thereby concluding the paper.

II. LITERATURE REVIEW: MAPPING THE FIELD AND IDENTIFYING THE GAP

The relevant scholarship papers are categorised into three broad clusters, each of which illuminates a different dimension of the problem and reveals a significant legal gap that no single body of writing has yet addressed.

A. THE THEORY OF DATA OWNERSHIP AND COMMODIFICATION (2015-2025)

European privacy law has the most sustained theoretical engagement with the question of personal data as property. Nadezhda Purtova's "The Illusion of Personal Data as no one's property" is an existing foundational work that argues that personal data is a resource of immense economic value. Still, the legal system has failed to define its ownership, hence enabling large tech platforms' advantage over individuals.[4] She further terms this asymmetry "data serfdom," in which individuals generate enormous value, but it is extracted without meaningful legal recourse.[5] Another scholar, Shoshana Zuboff, in her paper "The Age of Surveillance Capitalism, " argued that behavioural data derived from physical presence, movement and emotional state is the raw material of a new economic logic in which human experience is translated into predictable behaviour and sold as a commodity, hence extending the critique into a broader political economy. She has further identified emotional and physiological data as among the most valuable forms of behavioural extraction, contributing towards biometric AI, but her proposed idea is primarily political.[6] Some scholars believed that

[4] Nadezhda Purtova, *The Illusion of Personal Data as No One's Property*, 7 Law, Innovation & Tech. 83 (2015), https://doi.org/10.1080/17579961.2015.1052646

[5] *Id*. at 89-91.

[6] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* 8-10 (PublicAffairs 2019).

personal data should be treated as legal property, and one such scholar was Paul M. Schwartz, who argued for a framework with property rights in personal data to address the ownership gap between the people and the data about them that companies tend to monetise.

The individuals deserve the legal rights to control, sell, license or restrict the use of their personal information, which would in turn provide them with the leverage of dealing with companies as they would legally own the data.[7] While many scholars share a view similar to Paul Schwartz's, Lothar Determann counters this view, arguing that no one owns data and that any framework for it would obstruct information flow, thereby challenging the ownership model.[8] This data dividend existing literature from California and European civil society is tilted more towards a redistributed rather than a propertied solution, where the ownership rights are more like fiscal entitlement rather than a legal right. Hence, this paper aims to distinguish itself from such proposed regimes by proposing a judicially enforceable individual right rather than a policy mechanism.

B. INTELLECTUAL PROPERTY LAW AND BIOMETRIC TECHNOLOGY (2016-2025)

While the above school of thought was inclined almost entirely towards privacy law, contract, and political economy, and did not address the specific intellectual property dimension of the problem, a smaller but growing body of literature has emerged to examine biometric data through an IP lens. Elizabeth Rowe's work on trade secrets argues that the confidentiality model of trade secrets law is more suited to the sensitivity and uniqueness of biometric identifiers than the consent-and-breach model of privacy law.[9] But her argument serves relevance only to the company's interest to protect its database and not the individual's interest in the value extracted from their own characteristics.

Parineeta Goswami, on the other hand, has started interrogating whether biometric data can be treated as AI, implying that the existing IP categories are individually inadequate with respect to biometric data protection, as copyright requires creativity that biological generation cannot produce, and patents protect the technology of the biometric system and not the data itself. Trade secrets, as per the literature, protect the extractor's interest and not the concerned person's.[10]

This paper is built on the work of McSaty's Emotional AI and soft biometrics, which argues that the surveillance of emotional life constitutes a new form of biometric extraction for which neither privacy nor IP law has an adequate regime, hence attempts to develop the doctrinal vocabulary that this literature identifies as lacking.[11]

---

[7] Paul M. Schwartz, *Property, Privacy, and Personal Data,* 117 Harv. L. Rev. 2056, 2058-60 (2004).

[8] Lothar Determann, *No One Owns Data,* 70 Hastings L.J. 1, 3-7 (2018).

[9] Mary Wood, Why Your Face Should Be a Trade Secret, UVA L. (Mar. 23, 2023), https://www.law.virginia.edu/news/202303/why-your-face-should-be-trade-secret (reporting Elizabeth Rowe's arguments that facial and biometric data should receive protections comparable to trade secrets).

[10] Parineeta Goswami, *Biometric Data as Intellectual Property: Redefining Ownership in the Digital Age*, 3 NLUA J. Intell. Prop. Rts. 26 (2025).

[11] Andrew McStay, *Emotional AI, Soft Biometrics and the Surveillance of Emotional Life: An Unusual Consensus on Privacy*, 7 BIG DATA & SOC'Y, no. 1, 2020, at 2053951720904386, https://journals.sagepub.com/doi/full/10.1177/2053951720904386.

C. INDIAN DOCTRINAL SCHOLARSHIP ON DATA GOVERNANCE AND PERSONALITY RIGHTS (2018-2025)

The above-discussed literature does not address the Indian legal context and predominantly operates at a general theoretical level or engages with the US (BIPA) or EU (GDPR, AI Act) frameworks, hence creating a critical gap in the biometric IP theory with India's specific statutory architecture, such as the DPDP Act, Copyright Act, and personality rights jurisprudence.

Ever since the landmark judgment in the Puttaswamy case, Indian data governance has grown significantly.[12]

On personality rights, the case Anil Kapoor v. Simply Life India has contributed to the extension of publicity rights to AI-generated biometric exploitation as a significant doctrinal development. However, the case's ambiguity has not implied whether this judicial trajectory is a positive economic right in biometric data or merely a tortious remedy against misappropriation.[13] The work on AI training data by the Future of Privacy Forum and commentators such as Arora and Agarwal on voice biometrics has mapped the compliance implications of the DPDP Act for AI developers, but doesn't address any IP ownership questions, hence this paper aims to fill the gap that no existing work has succeeded in addressing (a) analysing IP theory to biometric data in the Indian Legal context, (b) proposed a positive doctrinal framework for biometric data ownership distinct from privacy and data protection theories or, (c) systematically address the personality rights jurisprudence as the foundation for a transferable economic right in biometric systems.

III. METHODOLOGY

The paper adopts a doctrinal methodology, employing a comparative analysis of statutory provisions, judicial decisions, and the internal logic of legal doctrines to determine whether and how they apply to novel factual situations. The comparative aspect of the paper focuses on three jurisdictions: the US (the Illinois Biometric Information Privacy Act and the right of publicity doctrine), the EU (the database directive, the GDPR, and the EU AI Act), and Japan (the amended unfair competition prevention act). Each jurisdiction is scrutinised for doctrinal relevance due to its legal response to a specific dimension of the biometric data ownership problem, offering a distinct model from that of India.

This paper does not employ empirical or socio-legal methods and makes a synthetic comparison identifying what each jurisdiction does well, what it fails to address and how such elements can be integrated into the Indian framework. The paper, like traditionally, does not survey the practices of AI developers nor quantify the commercial value of biometric training

[12] *Justice K.S. Puttaswamy (Retd) v. Union of India*, (2017) 10 S.C.C. 1 (India).

[13] *Anil Kapoor v. Simply Life India & Ors,.* 2023 SCC OnLine Del 6914 (India).

datasets, but proposes the doctrinal question: whether existing and proposed Indian law is capable of protecting biometric data ownership.

IV. ANALYSIS: THE THREE DOCTRINAL CANDIDATES AND THEIR STRUCTURAL FAILURES

A. THE COMMERCIAL LANDSCAPE: BIOMETRIC AI AND THE ECONOMICS OF THE SELF

Before moving on to the doctrinal question, it is necessary to understand that the biometric AI systems fall into three overlapping categories: facial recognition, voice and audio biometrics. The inhabited versus invented gap highly matters in practice because it demands attention towards the representation of both the commercial frontier and the most legally uncharted form of biometric extraction, where legal frameworks are most inadequate.

In India, facial recognition is deployed across the national automated facial recognition system maintained by NCRB, the DigiYatra airport passenger processing programme, including commercial-sector retail analytics, and access control systems.[14] Even in Voice Biometrics, startups have claimed to detect anxiety, depression, and cognitive decline from vocal biomarkers, further expanding into mobile banking authentication and call-centre fraud detection.[15]

Emotion AI infers psychological states from facial micro-expressions, tone, and even physiological signals; hence, it serves as the most legally urgent category to be protected. A lot of big companies have started commercialising emotion AI for hiring assessments, advertising testing and consumer behaviour research.[16] Scholars like Gremsl and Hödl have observed that emotional data does not merely identify a person but also extracts dynamic affective responses, also called soft biometrics, capturing their inner states at a given moment.[17] Now, a commercial assent of extraordinary value is built entirely upon such affective biometric data points when combined and trained upon and capable of predicting emotional responses across populations. For instance, consider a representative deployment scenario where an emotion AI hiring platform processes a video interview of a candidate and puts it through a facial action coding model that precisely records the facial movements. This unveils that the AI continuously tracks the facial features and behaviour, estimating emotions over time, such as anxiety, hesitation or confidence. This doesn't just

---

[14] Nat'l Crime Records Bureau, *National Automated Facial Recognition System: Functional Requirements Document* (2019) (India), panoptic.in; Ministry of Civil Aviation, *Digi Yatra Policy (DIGI YATRA)* (2022) (India), https://www.civilaviation.gov.in/sites/default/files/202307/Digi%20Yatra%20Policy%20%28DIGI%20YATRA%29.pdf.

[15] Anushka Choudhary & Surabhi Jain, *Biometric Data Regulation in India: Legal Landscape and Risks*, AZB & Partners (Feb. 14, 2024), https://www.azbpartners.com/bank/biometric-data-regulation-in-india-legal-landscape-and-risks/

[16] Gaudenz Boesch, *AI Emotion Recognition and Sentiment Analysis*, Viso.ai (Oct. 10, 2024), https://viso.ai/deep-learning/visual-emotion-ai-recognition/

[17] Thomas Gremsl & Elisabeth Hödl, *Emotional AI: Legal and Ethical Challenges*, 27 Info. Polity 163 (2022), https://doi.org/10.3233/IP-211529

happen with a single individual but with thousands of previous candidates whose patterns are compared with those already collected and labelled. The biometric AI training requires urgent addressal as the value extracted is from a collection of residue left behind by thousands of individuals whose inhabited features were derived without any explicit consent or acknowledgement.

The significance of a framework is twofold. First, a protective framework must be introduced to include identity markers, dynamic physiological signals and inferred psychological states that the current framework is not designed to address. Second, the sui generis framework must be designed to address the gap of individuals whose biometric value serves a commercial purpose.

B. COPYRIGHT AND THE ORIGINALITY PROBLEM

Section 13 of the COPYRIGHT ACT 1957 establishes the threshold condition of copyright, i.e. originality, where the Supreme Court in Easter Book Company v. D.B. Modak established that a work should reflect the author's own intellectual and creative effort.[18] With respect to such an established standard, the issue of biometric data protection faces a categorial barrier as it is generated by a biological process and not creative authorship, where there is no *invention but inhabitation.* A fingerprint, facial geometry, voice, none of these involves a human making choices about expression, selection or arrangement; rather, it emerges from genetics, laryngeal acoustics and other developments from which the copyright doesn't spring.

Section 2(o) of the Copyright Act, although it protects tables and compilations, does not, however, include the underlying biometric data.[19] As per the Eastern Book Company standards, the compilation should reflect intellectual effort in selection, arrangement or presentation, but a dataset of facial images from the internet involves no human intellectual selectivity, making it algorithmic, not authorial. Even where human curators label or select images, the copyright vests in the structure itself, giving individuals no copyright aspect in content that contains their faces or fingerprints. For example, if an Indian facial recognition company creates training datasets by deriving data from various social media profiles, and instead of AI, humans manually engineer those photos, the key question would remain the same, as the effort involved in removing duplicates and improving image quality is not creativity but technical tasks, hence doesn't qualify for the copyright protection criteria. Even if they manually engaged themselves in sophisticated decisions, copyright would, yet again, protect only the compilation, not the individual faces within it. Copyright law never protects the biometric information of individuals as their own right, but rather only as part of someone else's compiled dataset.

The existing copyright law belongs to the compiler and not the compiled person, as it rewards making but not vocabulary for *being*. The copyright act further lacks appropriate protection for the text-and-data mining exception contested through provisions of section 52, a gap now litigated in ANI Media Private Limited v. OpenAI Inc.[20]

---

[18] Copyright Act, No. 14 of 1957, § 13 (India); E. Book Co. v. D.B. Modak, (2008) 1 S.C.C. 1 (India).

[19] Copyright Act, No. 14 of 1957, § 2(o) (India).

[20] *ANI Media Pvt. Ltd. v. OpenAI OpCo LLC*, No. CS(COMM) 1028/2024 (Del. H.C.) (India) (pending).

The biometric ownership problem falls between two parallel conversations, where it is neither a purely copyright question nor purely a privacy one, based on the reference of DPIIT's 2025 working paper on AI and copyright, concerned with copyright holders' claims against AI developers.[21]

C. THE ABSENT DATABASED RIGHT: INDIA'S CRITICAL SUI GENERIS *LACUNA*

The sui generis right introduced by the EU's database directive of 1996 protects the database makers who have invested in obtaining, verifying, and presenting the database's contents when applied to biometric training datasets, protects companies that invest heavily in acquiring, labelling and verifying large biometric datasets against competitors who seek to free-ride.[22]

While this right is wholly independent of copyright, India, on the other hand, has no such framework as the Copyright Act 1957, which protects only the compilations through the originality threshold and no framework of investment-based protection like the EU.

The central point lies in the distinction of the proposed framework from the EU database right model, where the database right protects the extractor and not the persons extracted, protecting the AI companies better than the data subjects at all. No literature exists yet based on the data governance addressing such a lacuna, and further, the inhabited-versus-invented distinction reveals that the fundamental lacuna is the result of an absence of an instrument or framework recognising the person whose biological characteristics constitute the database's content as having an interest in the database at all. With respect to such a legal gap, Reddy and Chandrashekaran, although they identified the lacuna, further discussed it exclusively as investment protection for database makers.[23] The EU database right provides the base for protection of something that people invested substantial time, effort and money into, and just because it is a creative work, thus supporting the idea of creating a new legal framework that provides sufficient protection of valuable investments even when traditional authorship is difficult to identify.

D. PERSONALITY RIGHT AND THE PROPRIETORY SELF: AN INDIAN JUDICIAL GENEALOGY.

Indian courts have drawn inspiration from the US right-of-publicity doctrine, European moral rights tradition and constitutional privacy jurisprudence, developing a body of personality rights jurisprudence that recognises proprietary interests in an individual's identity, image, name and voice.

---

[21] Dep't for Promotion of Indus. & Internal Trade, Ministry of Com. & Indus/., Gov't of India, *Working Paper on Generative AI and Copyright Part 1: One Nation One License One Payment- Balancing AI Innovation and Copyright (Dec. 2025)* https://www.dpiit.gov.in/static/uploads/2025/12/ff266bbeed10c48e3479c941484f3525.pdf

[22] Council Directive 96/9/EC, art. 7, 1996 O.J. (L 77) 20 (EU). *Case C-202/12, Innoweb BV v. Wegener ICT Media BV*, ECLI:EU:C:2013:850, ¶¶ 52–54 (Ct. Just. Eur. Union Dec. 19, 2013).

[23] Prashant Reddy T. & Sumathi Chandrashekaran, *Create, Copy, Disrupt: India's Intellectual Property Dilemmas* (Oxford Univ. Press 2017).

ICC Development (International) Ltd. v. Arvee Enterprises serves as the foundation of recognising the right of publicity that gives the individual the right to license the use of their identity for commercial purposes.[24]

While Shivaji Rao Gaikwad v. Varsha Productions extended this protection to include physical characteristics, Anil Kapoor v. Simply Life India & Ors. took the decisive step, granting interim relief against the use of the name, image, voice and personality traits in AI-generated content, recognising right of publicity rights in biometric identity markers.[25]

This judicial precedent establishes three significant aspects relevant to the biometric ownership: Identity: physical and vocal characteristics carrying not only a privacy dimension but also a proprietary economic dimension.

The protection extends itself over exploitation through technological means, including AI and thirdly, in terms of all individual rights, the control over commercial exploitation of their identity. The framework for personality rights is not completely flawless and has three structural limitations that prevent it from serving as a full-fledged driver for biometric protection. First is the framework being the remedy against misappropriation and not really as a property right capable of licensing, transfer or inheritance, which makes it unsuitable for addressing the aggression of biometric training data extracted from millions of identities simultaneously. The same has been identified in Purtova's work on ownership and the property-rights approach to personal data.[26] Second is the recognition element of the publicity rights doctrine, which presupposes that the exploited characteristic is one by which the individual is publicly identified. Emotion AI systems derive value from aggregate statistical patterns, making the existing framework limited to individual recognisability rather than commercial reality. Third is the absence of a transferable economic right, as in India, the right of publicity framework is built on a quasi-moral-rights architecture. Rather than conferring a freely alienable economic asset, it primarily protects the dignity and autonomy in relation to identity.

Therefore, a more explicit and fundamentally strong property right is needed for biometrics to function as IP in a full economic sense capable of collective administration, licensing and revenue sharing.

V. THE INHABITED-VERSUS-INVENTED DISTINCTION AND THE CASE FOR A SUI GENERIS RIGHT.

A. THE THEORETICAL ARCHITECTURE

Having established that copyright, database protection and personality rights, including IP law's foundational assumption of a protectable subject matter being produced through human creativity and effort, fail to provide an adequate framework and basically render it incapable of addressing biometric data ownership. This legal gap

[24] Abanti Bose, *Personality Rights in Sports: ICC Development (International Ltd.) v. Arvee Enterprises & Anr.*, IPleaders (Aug. 25, 2021), https://blog.ipleaders.in/personality-rights-sports-icc-development-international-ltd-v-arvee-enterprises-anr/

[25] *Shivaji Rao Gaikwad v. Varsha Prods.*, 2015 SCC OnLine Mad 158, ¶ 12; *Anil Kapoor*, supra note 13, ¶ 34.

[26] Purtova, *supra* note 4, at 90-95.

requires a deep categorial framework addressing what IP law was designed for and what biometric data actually is.

Considering the internal logic of each IP right, biometric data fits into none of these paradigms. While copyright, patent and trademark protect subject matters that reflect authorship, an author's personality, creativity and product of branding, biometrics, on the other hand, are not invented but exist before and independently of any human intellectual act. It is a body and not a work signal sent by the rights holder to distinguish their good. It is a feature of the right-holder's body and hence not an invention, making it not a property at all as per IP law language.

Although biometric data serves a very similar role in the AI scenario, as mentioned above, it is treated entirely differently from IP. Like IP law subject matters, biometric data in AI training datasets can provide valuable information that is worth being collected, reproduced, processed and even monetised on a massive scale. The reason why biometric data is not protected by traditional IP law is that it's an aspect of the human body/identity that is not *invented* but rather *inherited.* While both the subject matters carry the same economic value, it is the distinction of the generative act that bars biometric data from being a part of IP law's protection subject.

Lothar Determann, in his work, argues an influential point: that no one owns data and that data is non-rivalrous, making it something no one can claim ownership of. According to him, creating a data rights regime would benefit large technology companies that possess enormous datasets under such a framework, rather than empowering individuals, and could strengthen the dominance of existing firms by enabling them to monetise such rights. This thesis doesn't merely mention Determann's argument but proposes a framework that overcomes the above concerns.[27] The framework proposed for biometric data is limited to the specific context of AI training and does not engage in its ability to be sold in perpetuity with waivers of privacy rights. The criticisms of a broad property right over personal data don't apply to the protection of biometric data because a sui generis, narrowly tailored regime for commercially exploited biometric data is significantly distinct from that of a property-personal data regime.

B. DISTINGUISHING THE PROPOSED FRAMEWORK FROM DATA OWNERSHIP AND COMMODIFICATION APPROACHES.

This part of the paper addresses the distinction between the proposed sui generis framework and the existing literature on data ownership and commodification. The central idea is that data as a property would allow people to sell their biometric data permanently, like any other subject matter, and this would exploit the economically vulnerable individuals.[28] Therefore, the proposed sui generis framework, based on the Illinois Biometric Information Privacy Act's prohibition on the sale of biometric identifiers, does not aim for full ownership but allows a limited revocable license that

[27] Determann, *supra* note 8, at 3-7.

[28] Schwartz, *supra* note 7, at 2058-60.

would preserve individuals' privacy rights, along with preventing permanent alienation of their biometric identity.[29]

The proposed framework is legally enforceable and not just another policy recommendation, framing the economic participating interest as a redistributive fiscal mechanism, requiring government implementation and not an individual legal right. None of the frameworks addresses this one critical gap: AI models are not built on the biometric data of a single individual but from thousands or millions of people, making the collective nature of biometric AI training that has been left unnoticed. The proposed framework seeks to address one of the biggest challenges for any property-based approach to personal data through a collective administration mechanism modelled on the copyright collecting societies established under Chapter VII of the Copyright Act, 1957.[30]

C. THE PROPOSED FRAMEWORK: A HYBRID SUI GENERIS MODEL

The proposed framework lays down four structural elements:

a) A right of economic participation: a non-waivable right to economic participation should be granted to every individual in the commercial exploitation of their biometric data as training input for AI systems, and includes data acquired directly or indirectly from secondary sources, such as internet images. This proposed right would derive its authority based on the artists' remuneration rights under section 38A of the Copyright Act 1957 and the WIPO Performers and Phonograms Treaty.[31] Practically, the moment an individual's facial geometry enters into an AI training pipeline, it acquires an entitlement which the DPDP Act's consent already governs but partially and aims to be paid for it like a musician earns royalties from a recording without any power over the distribution of the recording.

b) A collective administration mechanism: to see the reality, it is actually impractical to enforce rights against AI companies processing large amounts of biometric data. So to address the concern, the proposed framework would be designed in a similar structure to IPRS (IP Reference Substances) and PPL (Phonographic Performance Limited) through a Biometric Data Rights Society, which would further be supervised by a statutory authority with specific biometric AI expertise.[32] The process of granting biometric data for processing would work through section 6 of the DPDP Act while simultaneously registering with the society for economic participation purposes.[33] Like an AI developer would approach society as a large group to train a commercial biometric model without negotiating with every single individual, and the deal

[29] Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14/1-99 (2008).

[30] Copyright Act, No. 14 of 1957, §§ 33–36 (India).

[31] Copyright Act, No. 14 of 1957, § 38A (India); WIPO Performances and Phonograms Treaty art. 15, Dec. 20, 1996, 36 I.L.M. 76.

[32] *Indian Performing Right Soc'y Ltd. v. Eastern India Motion Pictures Ass'n*, (1977) 2 S.C.C. 820 (India).

[33] Digital Personal Data Protection Act, No. 22 of 2023, § 6 (India).

would be extended further after society calculates the royalties based on the category of biometric data used, and distribution would proceed periodically.

c) Non-waivability and minimum standards: the proposed sui generis regime should be non-negotiable, mandatory and non-waivable, which would prevent the companies from eliminating the rights through employment contracts, app terms of service or conditions for entering public or commercial spaces. This derives its approach from BIPA (Biometric Information Privacy Act) and section 6(4) of the DPDP Act to ensure that the individual retains their biometric data rights when dealing with powerful commercial actors.[34] For instance, this would require a fitness app to waive all the economic claims over the data collected through its camera-based tracker, foreclosing its terms of service and using the free tier of the service.

d) Integration with the EU AI Act as a compliance interface: AI developers designated under the EU AI Act's Annex III operating in India, deploying high-risk biometric systems, would be required to file a biometric data usage declaration with a designated authority to obtain a collective license under the society's administration.[35]

D. THE DOCTRINAL BASIS: RECOGNISING THE SELF AS A SOURCE OF RIGHTS IN BIOMETRIC INFORMATION

The Supreme Court's nine-judge bench in Justice K.S. Puttaswamy (Retd) v. Union of India recognised privacy as a fundamental right under Article 21.[36] Justice Chandrachud framed privacy as a foundational condition for individual autonomy and economic self-determination and not merely as a protection from intrusions. If the constitution already grants the people the right to control access to their biometric information, then the right to have a share in the value generated from their extracted data follows as a corollary grounded in the same constitutional commitment to dignity and autonomy.

Anil Kapoor's recognition has established that biometric characteristics are already understood by Indian courts as a source of legal rights and that AI -generated exploitation of biometric identity markers infringes personality rights. The ratio decidendi of Anil Kapoor's case, read along with Arvee Enterprises and Shivaji Rao Gaikawad, establishes the individual's relationship to their biometric characteristics upon which the proposed framework extends this judicial instinct from a tortious remedy to a positive economic right.

The DPDP Act has recognised biometric data as a defined category under section 2(t), thereby acknowledging that biometric data is constitutive of identity in a way that other

[34] Digital Personal Data Protection Act, No. 22 of 2023, § 6(4) (India).

[35] Regulation 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), arts. 5(1)(d)–(f), Annex III, 2024 O.J. (L 1689) 1 (EU).

[36] Puttaswamy, *supra* note 12.

categories are not, reflecting the act's differentiation between ordinary personal data and sensitive personal data.[37] The proposed sui generis framework is complementary to the DPDP Act as the former accepts the identity data's commercial value and provides the individual with legal rights to have a share in that value, whereas the latter can protect the privacy and regulate data processing.

VI. CONCLUSION

The paper has revealed a structural legal gap in India's intellectual property law, particularly regarding the deployment of biometric data in AI training systems, reflecting its inability to recognise the self as a subject matter of intellectual property rather than merely a subject of privacy.

The distinction between the inhabited and the invented is the paper's core argument, drawing on the idea that IP law protects what people make, not who people are. Biometric data extends beyond the body's surface to its psychological interior; hence, biometric data is what people are, not something generated by creative or inventive effort, but by their existence. The commercial value extracted from a person's inner life as training data for systems is immense and structurally immune to the existing legal order. The three doctrinal potential candidates failed due to the internal logic where biometrics lacked the authorship required by copyright, database protection lacked a sui generis form that would protect the extracted and personality rights that fail to address the aggregative, property-based protection, even when doctrinally promising cases exist like Puttaswamy, Arvee Enterprises and Anil Kapoor.

To formally integrate the proposed sui generis framework, it would require four legislative steps:

First, the amendment of the DPDP Act or introducing a separate statute for biometric data and its economic rights to include rights that would be triggered automatically where biometric data is used in commercial AI training under the parliament's authority. Second, the department for promotion of industry and internal trade should establish a biometric data rights society based on Chapter VII of the Copyright Act 1957, in coordination with the Ministry of Electronics and Information Technology, that would serve in parallel to IPRS with the power to prescribe royalty formulae for different biometric categories. Third, a non-waivability rule similar to that of the Illinois Biometric Information Privacy Act, where individuals would be asked to surrender their biometric protection rights to access a digital platform or any other service, rendering it legally void and unenforceable. This would prevent the take-it-or-leave-it contracts that large companies use to obtain broad rights over biometric data. Fourth, there should be a mutual recognition between the EU's AI Act for high-risk biometric AI systems and India's AI governance that would allow AI developers operating in any or both of the jurisdictions to meet India's proposed requirement as well as the EU's Annex III compliance

[37] Digital Personal Data Protection Act, No. 22 of 2023, § 2(t) (India).

obligations. This single regulatory process would significantly reduce compliance costs, making it easier for companies without any duplication of administrative requirements.

The proposed sui generis framework provides a doctrinal path that is aligned with the existing Indian legal materials, as it provides a right of economic participation, collectively administered with both the DPDP Act and the EU AL Act's high-risk classification system and also non-waivable. The framework is a synthesis of Indian law with its constitutional grounding in the Puttaswamy case, aligning with the personality rights and anchored in the DPDP Act's special treatment of biometric data. The deeper claim is about the protection of the individuals whose inhabited characteristics train the AI systems, but provide no credit for the value derived from their creators' biological characteristics. Hence, the law must develop instruments and further modify the IP law itself that can recognise the value of people, their body, voice, face and the emotional response and a failure to do so would result not only in a legal gap but a new form of enclosure of the self.