International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

The Evolving Domain of Privacy Rights: The Legal Challenges Posed by Emerging Biometric Data Collection Technologies

Mr. Abhinav Silakari

Assistant Professor, Law, LJ University

ABSTRACT

As 'automated' biometric data collection technologies like facial recognition, fingerprint scans, and iris tracking quietly become part of daily life, the boundary between convenience and intrusion is rapidly collapsing. Two decades ago, biometric technology was reserved to core areas such as forensics, crime-criminal identification procedures, and passports. The previous decade saw a boom in automation of biometric technology following the terrorist attacks, when countries like the United States, United Kingdom, India, and several others began authenticating via biometrics for the sake of national security. Fast forwarding to the present decade, biometric data collection technology has coupled with Artificial Intelligence, and is almost leading every aspect of our identities. Whether it is a simple legal procedure like Know-Your-Customer compliance or the act of unlocking a smartphone, it has gained access to the most intimate layer of a human-being's privacy. At this stage, it becomes imperative to ask: where should we draw the line? Can techno-legal boundaries genuinely reclaim personal privacy? The answers are convoluted.

The entire state of affairs has gone from identification to coerced authentication. In other words, identification that arose out of necessity has now become a requisite of proving one's identity to access basic human services, such as access to several Government schemes. The beauty of the entire issue at hand is that despite being nearly three decades old, it has, as it appears, successfully transitioned into the most concerning and troublesome threat to individual privacy. The article will focus on identifying the challenges that have surfaced, and the challenges that have potential to surface in the near future through biometric data collection technology, and how these categories can challenge the foundations of the law as it is known today. The analysis drawn as a consequence of this process will include scrutinized legislative steps, judicial precedents, and instances of comparative studies.

1. INTRODUCTION

As India paves the way for private entities to access Aadhaar based facial biometric authentication under Aadhaar Good Governance Initiative, it is prudent to apprehend that the step again draws attention to the long debated concern: that of biometric data collection tech and individual privacy.[1]

The term "biometric technology" is specifically defined under two legislations in India: The Information Technology (Reasonable security practices and procedures and sensitive personal data or information)

[1] *Notification of Aadhaar Authentication for Good Governance (Social Welfare, Innovation, Knowledge) Amendment Rules, 2025*, https://www.pib.gov.in/www.pib.gov.in/Pressreleaseshare.aspx?PRID=2098223 (last visited May 11, 2025).

Rules, 2011 (hereinafter, the Rules 2011), and the Aadhaar Act, 2016. Rule 2(1)(b) of the Rules of 2011 define "biometrics" as the technologies that measure and analyse characteristics of human body, including 'fingerprints', 'eye retinas and irises', 'voice patterns', "facial patterns', 'hand measurements' and 'DNA' for authentication purposes.[2] The definition widely covers almost every aspect of biometric technology used for the purposes of data collection. Another definition recognized by the legislation, defines "biometric-information" as photograph, finger print, Iris scan, or any other biological attributes of such kind and nature of an individual as may be specified by regulations.[3] The much recent Digital Personal Data Protection Act, (hereinafter, the DPDP Act) 2023, defines personal data, and often uses the term "sensitivity of personal data"[4]. The Bill of 2019 unhesitantly placed the biometrics in the "sensitive personal data" category.[5]

However, the latest attempt to safeguard citizens' digital rights and iron-guard their personal data abstractly defines personal data and leaves a wide room for the Union to amend the Act's definition clause in later amendments. The term "personal data" under the DPDP Act is defined as any data about an individual through which he may be identifiable.[6]

For the purposes of this article, the term biometric technology, including but not limited to the term biometric data collection technology, shall mean to address the automated technology, unless context expressly provides otherwise. The following chapters in the article will examine India's legal framework; from constitutional principles and landmark court rulings to the three statutes dealing with the key questions of biometric systems, data collection, and privacy, including the Aadhaar Act, IT Act, and the new DPDP Act. The analysis drawn will be in the context of mass automated biometric data collection. It will critically present issues of non-transparency, data misuse, accountability gaps and surveillance architecture, and draw occasional contrasts with Europe's GDPR and U.S. regulatory approaches.

2. PRIVACY AS UNDER THE CONSTITUTION

The growing ubiquity of biometrics has raised serious alarm bells about privacy, transparency, and consent. In India, hundreds of millions of people now have some biometric data on record (through Aadhaar), often without fully understanding how it will be used or shared. The concerns were ideally dealt with in the two Puttaswamy judgements. It would be ideal to refer to these in the given light.

Privacy as a Fundamental Right and "Informational Self-Determination"

India's Supreme Court declared in *K.S. Puttaswamy v. Union of India*[7], that privacy is a fundamental right under Article 21 of the Constitution. Importantly, the Court recognized an individual's informational

[2] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, Rule 2(1)(b)

[3] The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, § 2(1)(g), https://uidai.gov.in/images/Aadhaar_Act_2016_as_amended.pdf.

[4] *The Digital Personal Data Protection Bill, 2023*, PRS Legislative Research, https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023 (last visited May 11, 2025).

[5]The Personal Data Protection Bill, 2019, Bill no. 373 of 2019, § 3(7), *Personal Data Protection Bill, 2019.Pdf*, https://prsindia.org/files/bills_acts/bills_parliament/2019/Personal%20Data%20Protection%20Bill,%202019.pdf (last visited May 11, 2025).

The Bill was withdrawn and the new DPDP Bill, 2023, was introduced in Lok Sabha, and enacted in the same year.

[6] The Digital Personal Data Protection Act, 2023, § 2(t), *Digital_Personal_Data_Protection_Act,_2023.Pdf*, https://prsindia.org/files/bills_acts/bills_parliament/2023/Digital_Personal_Data_Protection_Act,_2023.pdf (last visited May 11, 2025).

[7] AIR 2017 SC 4161, *Justice K.S.Puttaswamy(Retd) And Anr. vs Union Of India And Ors. on 24 August, 2017*, https://indiankanoon.org/doc/91938676/ (last visited May 11, 2025).

privacy, in other words, the right to control personal data, as intrinsic to dignity and autonomy. Justice Chandrachud's dissent in *Puttaswamy II* (the Aadhaar case)[8] reiterated that "access to personal data of an individual must be governed by a legal regime built around the principles of consent, transparency, and individual control"[9] The nine-judge bench explicitly urged the legislature to put in place a "carefully structured regime" for personal data protection.[10] In other words, India's highest court demands robust safeguards (legal standards, oversight, consent mechanisms) for handling biometric and other personal data. Any infringement on informational privacy must satisfy a strict test of legality, legitimate aim and proportionality.[11] However, these lofty principles have yet to fully materialize into effective practice. In the Aadhaar case, the majority accepted that a government-run biometric database could advance welfare goals, so long as collection was minimal and time-limited.[12] The Court observed that Aadhaar's architecture "is not necessarily conducive to creating a surveillance State," noting safeguards like encryption and limited storage.[13] Dissenting Justice Chandrachud, by contrast, warned that Aadhaar embodied "bio-potential" – once biometrics are compromised, they are "compromised forever".[14] This tension highlights India's legal crossroads: recognition of privacy as fundamental versus acceptance of vast biometric systems for governance, as highlighted in the later sections of this article.

3. THE STATUTORY DISAPPOINTMENT

Aadhaar: The Double-Edged Biometric ID

India's Aadhaar program (enacted via the Aadhaar Act 2016) sets the clear tone for the country's biometric ambitions. It has assigned a 12-digit identity number to over 1.4 billion residents, each linked to fingerprint and iris scans.[15] Aadhaar was originally touted to target social welfare effectively. Indeed, the Supreme Court ultimately upheld Aadhaar's use for state subsidies and benefits as constitutionally valid, recognizing it could empower the marginalized by curbing leakages.[16] However, this centralized database also precipitated privacy nightmares. Over time, governments linked Aadhaar to many services: from bank accounts and mobile connections to school admissions. Crucially, in the Aadhaar *case* the Court strictly limited the Act's reach. It struck down Section 57 of the Aadhaar Act, which had allowed private companies to use Aadhaar authentication or eKYC, even by mere contractual arrangement.

The majority noted that permitting "any body corporate or person" to demand authentication on contract basis would enable "commercial exploitation" of citizens' biometric/demographic data, thereby impinging privacy.[17] Justice Sikri's opinion made clear: *"There cannot be any use of Aadhaar authentication or E-KYC by private companies for any purpose whatsoever."*[18]

---

[8] AIR 2018 SC (SUPP) 1841, *Justice K.S.Puttaswamy(Retd) vs Union Of India on 26 September, 2018*, https://indiankanoon.org/doc/127517806/ (last visited May 11, 2025).

[9] *Id.*

[10] *Constitutionality of Aadhaar Act: Judgment Summary*, Supreme Court Observer, https://www.scobserver.in/reports/constitutionality-of-aadhaar-justice-k-s-puttaswamy-union-of-india-judgment-in-plain-english/ (last visited May 11, 2025).

[11] Justice K.S.Puttaswamy(Retd) vs Union Of India on 26 September, 2018, *supra* note 8.

[12] *Id.*

[13] *Id.*

[14] Gautam Bhatia, *The Aadhaar Judgment: A Dissent for the Ages*, Constitutional Law and Philosophy (Sep. 27, 2018), https://indconlawphil.wordpress.com/2018/09/27/the-aadhaar-judgment-a-dissent-for-the-ages/.

[15] *supra* note 3, § 3

[16] Constitutionality of Aadhaar Act, *supra* note 10.

[17] Justice K.S.Puttaswamy(Retd) vs Union Of India on 26 September, 2018, *supra* note 8.

[18] *Id.*

Consequently, after 2018, no private entity can legally compel Aadhaar-based KYC unless a specific law permits it. (The government did amend Section 57 to remove the phrase "or any contract," allowing private use only if explicitly authorized by the legislation. Once the judgement came into effect, the developments post 2018 were noteworthy, and striking, however inadequate, as is highlighted in the following segment.

Attempted Responsive Developments

To its credit, UIDAI did introduce certain technical fixes post-2017, such as the Virtual ID (VID) system and Limited KYC mechanisms to reduce exposure of Aadhaar numbers and limit biometric data reuse.[19] Encryption standards were enhanced, and UIDAI claimed to enforce server isolation.[20] However, independent audits (such as the CAG report of 2022) exposed enforcement loopholes: poor compliance by Authentication User Agencies (AUAs), lack of timely audits, and failure to ensure that earlier clients weren't storing biometric data.[21]

The legal framework, thus, remains structurally imbalanced. The judiciary called for strong, citizen-centric privacy protections; the executive responded with bureaucratic insulation, rather than rights-based reform.[22] The Aadhaar infrastructure continues to expand—now into the private domain—without constitutional recalibration.[23]

Data Protection and Privacy Law: A broader outlook outside the biometrics

Before 2023, India lacked a dedicated data protection statute. The Information Technology Act, 2000 (hereinafter, the IT Act) and related rules provided modest safeguards.[24] Under the IT Rules 2011, biometric data was classified as "sensitive personal data," meaning companies handling it should implement precautions.[25] Section 43A of the IT Act (introduced in 2008) even required corporate entities to compensate users if negligence caused a data breach.[26] Legislatively, the much-anticipated Digital Personal Data Protection (DPDP) Act, 2023, was passed. It introduces user consent mechanisms and creates a Data Protection Board.[27] However, it frequently grants blanket exemptions to the State under the veil of "public order" or "national interest."[28] The lack of enforceable rights or a compensation mechanism

[19] *What Are the Data Protection and Privacy Measures Taken by UIDAI?*, Unique Identification Authority of India | Government of India, https://uidai.gov.in/en/289-faqs/your-aadhaar/protection-of-individual-information-in-uidai-system/1943-what-are-the-data-protection-and-privacy-measures-taken-by-uidai.html (last visited May 11, 2025).

[20] *Id.*

[21] Dr Gopal Krishna, *CAG's audit report creates a case for dismantling of UIDAI and scrapping of Aadhaar project*, Junputh (May 1, 2022), https://english.junputh.com/lounge/cag-performance-audit-of-functioning-of-uidai-is-partial-and-incomplete/.

[22] *CJI: Executive's Tendency to Ignore Court Orders a Worry | India News - Times of India*, https://timesofindia.indiatimes.com/india/cji-executives-tendency-to-ignore-court-orders-a-worry/articleshow/88511609.cms (last visited May 11, 2025).

[23] Notification of Aadhaar Authentication for Good Governance (Social Welfare, Innovation, Knowledge) Amendment Rules, 2025, *supra* note 1.

[24] Editoral Team, *Grey Areas of IT Act 2000 – Legal Challenges and Solutions*, LawCrust Global Consulting Company (Dec. 12, 2024), https://lawcrust.com/grey-areas-it-act-2000/.

[25] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, Rule 3 (vi) https://www.indiacode.nic.in/handle/123456789/1362/simple-search?query=The%20Information%20Technology%20(Reasonable%20Security%20Practices%20and%20Procedures%20and%20Sensitive%20Personal%20Data%20or%20Information)%20Rules,%202011.&searchradio=rules (last visited May 11, 2025).

[26] *It_act_2000_updated.Pdf*, https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf (last visited May 11, 2025).

[27] Digital_Personal_Data_Protection_Act,_2023.pdf, *supra* note 6.

[28] *Digital Personal Data Protection Act, 2023: A Missed Opportunity for Horizontal Equality*, Supreme Court Observer, https://www.scobserver.in/journal/digital-personal-data-protection-act-2023-a-missed-opportunity-for-horizontal-equality/ (last visited May 11, 2025).

in case of biometric misuse leaves users structurally powerless—especially against the State.[29] For instance, it repeals section 43A of the IT Act which empowered the citizens, including vulnerable groups, in terms of autonomy breach over personal data.[30] Previously Section 43A of the IT Act had allowed damages for negligence; now, only administrative penalties (up to ₹250 crore) can be imposed on offending entities, but none of that fine compensates users.[31]

In theory, the DPDP Act imposes new requirements on "data fiduciaries" (entities handling digital personal data):[32] they must obtain consent or identify a legitimate ground before processing, limit data to specified purposes, ensure accuracy, allow individuals rights of access and erasure, and report breaches.[33] The Act even draws on GDPR-like norms: for example, it broadly defines personal data and grants a data principal (individual) rights to information and erasure.[34] In practice, however, the DPDP Act has garnered sharp criticism for gaping loopholes and executive overreach.[35] The official summary observes that the Act creates a "Data Protection Board of India" with powers to investigate and fine, yet that Board cannot issue binding regulations or guidance.[36]

More concerningly, the Act carves out extensive exemptions for government agencies.[37] In effect, the government can exempt itself from core obligations. Critics note, for instance, that Section 7(b) lets public authorities bypass consent and purpose-limitation requirements altogether.[38]

Other shortcomings have been pointed out: nearly 26 instances of "as may be prescribed" litter the Act, meaning crucial details (e.g. definitions, exemptions) will be filled in later by rule-making.[39]

Section 17(2) goes further, providing the Union government blanket immunity to process any data for national security, maintenance of public order, sovereignty, etc., without being bound by the Act.[40] Such provisions risk creating "a segregated sphere of activities positioned outside the jurisdiction of data privacy norms," thus imperatively enabling mass surveillance unchecked by law.[41] The requirement for consent was weakened – fiduciaries no longer must fully explain to data principals how long data is retained or which third parties will receive it.[42]

In short, while the DPDP Act finally enshrines privacy as a right and brings India in line with global norms on paper, experts warn it falls short in practice. It leans heavily on exemptions and delegated rule-making. For example, media and civil society have noted that an amendment to India's Right to Information Act

[29] Akshay Dhekane, Urvashi Singh & Akshay Dhekane and Urvashi Singh, *Weakened Right to Access: How DPDP Act Limits Your Control Over Personal Data – Part I*, Law and Other Things (Oct. 31, 2024), https://lawandotherthings.com/weakened-right-to-access-how-dpdp-act-limits-your-control-over-personal-data-part-i/.
[30] Digital Personal Data Protection Act, 2023, *supra* note 28.
[31] Digital_Personal_Data_Protection_Act,_2023.pdf, *supra* note 6, Schedule, § 33(l)
[32] *Id.*
[33] *Id.*
[34] *Id.*, § 4, 5, 6
[35] Dhekane, Singh, and Singh, *supra* note 29.
[36] Digital_Personal_Data_Protection_Act,_2023.pdf, *supra* note 6, § 27, 28, 29
[37] *Id.*, § 17
[38] *The Right to (Pry)-Vacy: Understanding India's Dystopian Data Protection Legislation – NYU JILP*, (Feb. 12, 2024), https://nyujilp.org/the-right-to-pry-vacy-understanding-indias-dystopian-data-protection-legislation/.
[39] *Id.*
[40] Digital_Personal_Data_Protection_Act,_2023.pdf, *supra* note 6, § 17(2)
[41] The Right to (Pry)-vacy, *supra* note 38.
[42] Sarvesh Mathi, *Fifteen Major Concerns with India's Data Protection Bill, 2023*, MEDIANAMA (Aug. 4, 2023), https://www.medianama.com/2023/08/223-major-concerns-india-data-protection-bill-2023-2/.

(through the DPDP Act) now broadly exempts "personal information" from disclosure,[43] which is a subtle change that undermines governmental transparency and public accountability. Overall, India's new data protection regime marks progress, but underplays the safeguards – especially for sensitive biometric data – that many had hoped for.

4. GOVERNMENT SURVEILLANCE & BIOMETRIC INFRA

After arguing as to what are the statutory deficiencies that make superimposition of biometric authentication risky, it is now ideal to understand how these steps may lead to enhanced surveillance. The legal debates above matter because the Indian state is aggressively deploying biometric surveillance.[44] Various arms of government now collect and use biometric data, often under vague legal authority. For example, the Criminal Procedure (Identification) Act, 2022 (amending earlier laws) explicitly empowers police to collect an expanded suite of biometric and physical data from convicts and suspects – from iris scans to facial images and voice samples. Media reports note this sweeping power was enacted at the same time India lacked any comprehensive privacy law, raising urgent concerns.[45] Police forces across the country have rolled out facial recognition technology (FRT). The Delhi Police, for example, maintain a facial database (drawn from ID Act photographs) and claim to scan CCTV feeds during riots and major events. In practice, however, FRT use has been shrouded in opacity. An RTI by the Internet Freedom Foundation found that the Delhi Police consider even low-confidence face matches as "false positives" that warrant investigation.[46] In other words, even a 20–30% similarity score does not clear a person; police records show they still subject such matches to further probing. The approach can ensnare innocents: "people with the slightest facial similarity can be targeted," potentially stigmatizing minority communities.[47]

Elsewhere too, state governments are embracing biometric surveillance. Tamil Nadu's police deployed an FRT portal built by a local tech institute, though it initially lacked clear "suspect criteria."[48] That portal was hacked in 2024: a data breach exposed ~800,000 records from the system, including names, phone numbers, FIR details and presumably facial images of individuals flagged by police.[49] The hack (by a group called "Valerie") illustrates the vulnerability of keeping a centralized face database. The Tamil Nadu incident was not isolated: a 2024 report exposed a 500 GB cloud data leak of a contractor's server containing fingerprints, facial images, job applications and even tattoos and scars of thousands of police and military personnel.[50]

---

[43] *DPDP Does Not Weaken RTI Act: Union Minister Ashwini Vaishnaw*, The Economic Times, Apr. 10, 2025, https://economictimes.indiatimes.com/tech/technology/dpdp-does-not-weaken-rti-act-union-minister-ashwini-vaishnaw/articleshow/120168627.cms?from=mdr.

[44] *India's Surveillance Landscape after the DPDPA | IAPP*, https://iapp.org/news/a/india-s-surveillance-landscape-after-the-dpdpa (last visited May 11, 2025).

[45] Vallari Sanzgiri, *80% Accuracy in Facial Recognition (FRT) Is Enough for Delhi Police*, MEDIANAMA (Aug. 18, 2022), https://www.medianama.com/2022/08/223-delhi-police-iff-rti-facial-recognition-80-percent-accuracy-2/.

[46] *Id.*

[47] *Id.*

[48] Joel R. McConvey, *Indian Police Adopt Facial Recognition despite Risk of Massive Data Breaches | Biometric Update*, (May 7, 2024), https://www.biometricupdate.com/202405/indian-police-adopt-facial-recognition-despite-risk-of-massive-data-breaches.

[49] *Id.*

[50] *A Leak of Biometric Police Data Is a Sign of Things to Come | WIRED*, https://www.wired.com/story/police-face-recognition-biometrics-leak-india/ (last visited May 11, 2025).

These cases show that Indian law enforcement accumulates biometric "honeypots," and even well-guarded police systems can spill out highly sensitive personal data. The instances of fraud and identity theft (where the hijackers now have the raw data to impersonate victims) are rather dangerously placed. The Center has also flirted with a national facial-recognition system (AFRS). Privacy advocates vocally oppose this. An Amnesty campaign called "Ban The Scan" stresses that India's AFRS "contemplates a nationwide centralized database that will enable State actors to track your every move – in the absence of basic privacy, security and rights protections."[51] Amnesty warns that FRT can "amplify discriminatory policing" of marginalized groups.[52] and that errors (Delhi Police's test run matched a missing woman only 2% of the time) can ruin innocent lives. Despite such red flags, state governments continue deploying FRT cameras, for instance, the State of Meghalaya plans to install 300 cameras in Shillong.[53] In essence, India has built a sprawling biometric surveillance architecture – courts and laws have yet to catch up with how to regulate it.[54]

A Tale of Consent, Transparency, and Data Misuse

A central concern with automated biometric collection is the dearth of informed consent and transparency. Often, individuals are not told how their biometrics will be processed, who can access them, or how long they will be stored. For instance, Aadhaar enrolment requires agreeing to biometric capture, but subsequent uses (e.g. linking your ID to a ration card or bank account) are framed as mandatory by government rule rather than true choice.

The instance, as mentioned earlier, hints at the aspect of coerced authentication rather than informed consent. And the statement is not a desperate critique of the advancement initiative. However, it is inquisitive to ask: where lies the line of difference; between a wrapped up coerced consent and informed free consent when everything is mandated and deemed necessary? And, to put it simply, is this correct in the eyes of the law?

Even when consent is nominally obtained (say, clicking "agree" on an app), research shows most users do not grasp the downstream uses. The new DPDP Act mandates a simple "notice" at the time of collecting consent, but that notice need only specify *what* data is collected and *broadly* why – it need not enumerate the specific recipients, retention period, or your right to lodge a complaint.[55]

In practice, this weak regime means users have little real understanding or control. That opacity feeds the risk of secondary uses and misuse. Biometric data can be easily repurposed once collected. People may give consent for a narrowly defined purpose, but their biometrics might later be used for profiling or cross-matching with other databases.[56] Indeed, cases of Aadhaar-enabled fraud show what can go wrong: the Ministry of Home Affairs reported over 29,000 instances of Aadhaar-enabled payment (AePS) fraud in 2024.[57]

[51] *Hyderabad*, https://banthescan.amnesty.org/hyderabad/index.html (last visited May 11, 2025).
[52] *Id.*
[53] McConvey, *supra* note 48.
[54] Krishna Ravi Srinivas, *Two Reasons AI Is Hard to Regulate: The Pacing Problem and the Collingridge Dilemma*, The Hindu, May2, 2023, https://www.thehindu.com/sci-tech/science/ai-regulation-pacing-problem-collingridge-dilemma/article66802967.ece.
[55] Mathi, *supra* note 42.
[56] *Biometric Data: Why Is It Problematic?*, https://www.mondaq.com/india/data-protection/1508150/biometric-data-why-is-it-problematic (last visited May 11, 2025).
[57] *Id.*

Criminals used cloned or stolen fingerprints and Aadhaar details to siphon money from accounts.[58] This "biometric cloning" means that breaches can have direct financial harm.[59] Furthermore, there is virtually no effective oversight of how biometric data flows. An illustrative hypothetical example is as follows: state police might share fingerprints with central databases without any public notice. Companies can harvest facial images from social media without consent – in practice, many tech firms train AI models on large image corpora scraped from the web.[60] Because India's regulatory machinery is nascent, such practices often go unchecked.[61] In sum, the combined effect is a system that lacks meaningful checks: citizens rarely have a real chance to refuse biometric collection, rarely know how long data is kept or who it's shared with, and have no guarantee the data won't be misused. Activists caution that even well-intentioned systems become invasive "in the absence of basic privacy, security and rights protections."[62] When the state or big corporations wield powerful AI-based biometrics, the potential for mission creep and consequent abuse is enormous.

High-Profile Breaches Illustrate Vulnerabilities

Real-world incidents have already highlighted the perils. In late 2023, cybersecurity firm Resecurity discovered that Aadhaar and other personal data for 81.5 crore Indians was being offered on the dark web.[63] The leaked dump (sourced from an ICMR COVID-19 database) included names, phone numbers, addresses, Aadhaar numbers and passport details of tens of millions. As reported, it was "possibly the 'biggest' case of data leak in the country."[64]

Such a breach shows how Aadhaar-linked data (beyond biometrics) can leak via other data collections. Once Aadhaar numbers are exposed at scale, it can facilitate identity theft and fraudulent use of biometric authentication systems. Law enforcement biometric systems have also been compromised. We noted the Tamil Nadu FRT breach above.[65] Crucially, biometric identifiers stolen in these ways cannot be changed like a password or ID card can; once they're out in the open, the victims have no easy recourse.[66]

These breaches underscore ethical questions: should we entrust sensitive traits to any system that may be attacked? The evidence suggests we must tread cautiously either way. But is it achievable in case of coerced consent as questioned above? What if one loses the opportunity to avail government benefits? As simple as these questions may sound, each requires a legislative thought and executive action.

Each breach of biometric data exponentially increases the risk of fraud (as the data can be cloned or spoofed) and profiling.

---

[58] *CASES OF BIOMETRIC CLONING FOR FINANCIAL FRAUD*, https://www.pib.gov.in/www.pib.gov.in/Pressreleaseshare.aspx?PRID=2039647 (last visited May 11, 2025).

[59] *Id.*

[60] *Privacy Concerns in the Age of AI: The Risks of Biometrics and Personal Data Usage | by Rajesh Devadasan | Apr, 2025 | Medium*, https://medium.com/@rajeshdevadasan/privacy-concerns-in-the-age-of-ai-the-risks-of-biometrics-and-personal-data-usage-344bec15fbfc (last visited May 11, 2025).

[61] Srinivas, *supra* note 54.

[62] Hyderabad, *supra* note 51.

[63] HT News Desk, *Aadhaar Details of 81.5 Cr People Leaked in India's 'Biggest' Data Breach*, Hindustan Times (Oct. 31, 2023), https://www.hindustantimes.com/technology/in-indias-biggest-data-breach-personal-information-of-81-5-crore-people-leaked-101698719306335.html.

[64] *Id.*

[65] McConvey, *supra* note 48.

[66] A Leak of Biometric Police Data Is a Sign of Things to Come | WIRED, *supra* note 50.

Under current law, victims have little legal remedy. Even the DPDP Act's breach-reporting requirements only compel the controller to notify affected users; they do not guarantee compensation.[67] This leaves ordinary citizens highly exposed with limited legal protection if their biometrics leak.

5. SOME NOTEWORTHY CRITICISM AND GAPS IN INDIAN LEGAL FRAMEWORK

In light of the above, experts and civil society have leveled scathing criticisms at India's biometric regime and privacy laws. Some of the key concerns include:

One, the DPDP Act and related laws grant the state sweeping exemptions from privacy rules. Analysts note that Indian legislation repeatedly allows state agencies to sidestep consent, purpose limitations, and even entire sections of the law.[68]

Two, the lack of opportunities for people to challenge the legislative attempts to mandate biometric authentication undermines the Constitution's checks and balances: e.g. the legislature itself was circumnavigated when Aadhaar was enacted as a money bill in 2016, an issue which Justice Chandrachud raised as "debasement" of Parliament.[69] In any event, the net effect is that citizens have almost no way to challenge or even know about the government's use of their biometric data in sensitive areas.

Three, privacy advocates point out that many biometric collections happen without genuine choice. When linking Aadhaar became quasi-mandatory for everything from bank accounts to SIM cards, individuals rarely had an alternative. Similarly, CCTV-based facial scans happen without notice or opt-out. The DPDP Act purports to base processing on consent or a legal ground, but its actual consent provisions are toothless – companies can share data widely after a user "opts in" without the user knowing whom they're trusting. The absence of meaningful choice violates the ideal of autonomy that *Puttaswamy* enshrined.[70]

Four, even though India now has a data protection law, it lacks a truly independent regulator with enforcement teeth. The Data Protection Board is government-appointed and cannot issue regulations or enforce criminal penalties.[71] There is no privacy ombudsman or tribunal to adjudicate individual grievances. In practice, breaches and violations are mostly addressed via media scrutiny or lobbying rather than robust legal accountability. By contrast, GDPR regimes give citizens a direct private right to sue and strong fines that partly compensate victims – protections that India's law currently omits.[72]

Five, a corollary is that the public is largely in the dark about how biometrics are used or misused by both state and companies. Note the Delhi Police's refusal to disclose basic facts about FRT accuracy or usage that we discussed above.[73] Neither Aadhaar nor DPDP requires proactive transparency reports on government access to data. Victims of misuse (say, being incorrectly flagged by a face-match) have no clear remedy to challenge decisions or seek recourse, beyond filing broadly framed writ petitions.

Six, despite being especially sensitive, biometric data in Indian law has not been given truly heightened protection. Under GDPR, biometric data "for the purpose of uniquely identifying a person" is a special category of data, whose processing is flatly prohibited unless exceptions (like explicit consent or vital

[67] Mathi, *supra* note 42.
[68] The Right to (Pry)-vacy, *supra* note 38.
[69] Constitutionality of Aadhaar Act, *supra* note 10.
[70] Mathi, *supra* note 42.
[71] Dhekane, Singh, and Singh, *supra* note 29.
[72] India's surveillance landscape after the DPDPA | IAPP, *supra* note 44.
[73] Sanzgiri, *supra* note 45.

interests) apply.[74] India's DPDP Act does not specify "biometric" as a special category. While it generally restricts processing to stated purposes, it does not ban, say, police scanning your face from a camera feed without court oversight. Critics have noted that India's law stopped short of the GDPR's strong stance; for example, Section 9 of the DPDP Act could have listed biometric as a "sensitive" category requiring additional consent, but it did not.[75]

Lastly, India also has unique data transfer rules, but they are still evolving. The DPDP Act is unclear on whether biometrics can be transferred abroad or held in offshore servers. Pending rules on cross-border transfers may leave gaps in securing biometric data processed by multinational tech firms.[76]

To sum up this chapter, India's privacy framework currently has many grey zones. No law yet prevents law enforcement from deploying FRT in public without a warrant (as some European countries require). There is no statutory limit on how long government authorities can retain biometric data. Corporate non-compliance (e.g. a company secretly monetizing face scans) risks only a fine, not a prison term. And the path for judicial review is murky: Indian courts have not yet squarely addressed questions like whether *any* FRT by police violates *Puttaswamy*.

6. GLOBAL PERSPECTIVES AND EMERGING DEBATES

For context, it is instructive to contrast India's approach with international norms. The European Union's GDPR, 2018, regards biometric data used for identification as especially sensitive.[77] Consent must be "explicit," meaning individuals must be clearly informed and voluntarily agree. Even then, most GDPR jurisdictions require additional safeguards. The EU's AI Act severely restricts use of high-risk AI systems (like public facial recognition) unless strict conditions are met.[78] In short, the EU's stance is precautionary: biometric surveillance is only allowed under narrow, transparent rules, with robust data subject rights. India's law nominally echoes some GDPR principles (e.g. data minimization, erasure rights) but falls short of GDPR's explicit color-coded protections. For example, GDPR mandates Data Protection Impact Assessments for large-scale biometric profiling; India's DPDP Act says nothing comparable. In the United States, there is no comprehensive federal data protection law. Instead, several states regulate biometrics. Illinois's Biometric Information Privacy Act (BIPA) is the most stringent: it requires private entities to obtain written consent before capturing any biometric identifier (including scans of face, fingerprints, retina, etc.), specify retention periods, and delete data after use.[79] BIPA also creates a private right of action, and in a recent high-profile litigation, Facebook agreed to a $650 million settlement for allegedly collecting users' faceprints without consent.[80] Texas and Washington have similar, albeit weaker, biometric privacy statutes.

---

[74] *Art. 9 GDPR – Processing of Special Categories of Personal Data*, General Data Protection Regulation (GDPR), https://gdpr-info.eu/art-9-gdpr/ (last visited May 11, 2025).

[75] *The Digital Personal Data Protection Act of India, Explained - Future of Privacy Forum*, https://fpf.org/, https://fpf.org/blog/the-digital-personal-data-protection-act-of-india-explained/ (last visited May 11, 2025).

[76] *Cross Border Data Transfers under the DPDP Act*, https://www.leegality.com/consent-blog/cross-border-data-transfer (last visited May 11, 2025).

[77] Art. 9 GDPR – Processing of special categories of personal data, *supra* note 74.

[78] *Section 1: Classification of AI Systems as High-Risk | EU Artificial Intelligence Act*, https://artificialintelligenceact.eu/section/3-1/ (last visited Apr. 14, 2025).

[79] *Biometric Information Privacy Act (BIPA) | ACLU of Illinois*, (Apr. 26, 2021), https://www.aclu-il.org/en/campaigns/biometric-information-privacy-act-bipa.

[80] *Facebook's $650M BIPA Settlement 'a Make-or-Break Moment' | IAPP*, https://iapp.org/news/a/facebooks-650m-bipa-settlement-a-make-or-break-moment (last visited May 11, 2025).

California's Consumer Privacy Act and its successor (CPRA) classify biometrics as "sensitive personal information" that consumers can opt out of sharing.[81] At the federal level, Congress has introduced various privacy bills (for instance, the American Privacy Rights Act, or more recent federal data/privacy proposals[82]), but none have passed yet. Thus, U.S. debates continue on whether to follow the European model or defer to sectoral regulation.

For India, the lesson is clear: GDPR-style rules offer one model – strong protections, heavy fines, independent regulators – whereas the U.S. model relies on targeted laws and litigation. India's DPDP Act leans toward an EU-like framework on paper, but the numerous carve-outs and weaker enforcement echo the "toothlessness" critics charge of U.S. self-regulation. In conclusion, India's struggle will be whether it can balance its developmental and security priorities with the civil liberties that established democracies still strive to protect in this new era of mass biometrics.

7. CONCLUSION

Automated biometric data collection – from Aadhaar's fingerprints to city-wide facial recognition networks – has undoubtedly become a defining feature of India's digital landscape, for it not only offers a monotonous global solution, but the protective legal framework offers a little help. The scenario could be even worse were the victims from vulnerable groups. These technologies promise efficiency and security, but they also create unprecedented risks. India's evolving legal response has been uneven. On one hand, the Constitution's privacy guarantee, reinforced by *Puttaswamy* and other rulings, provides a strong theoretical bulwark. On the other hand, statutory law has often ceded ground: Aadhaar came into existence under a Money Bill without full parliamentary debate; the IT Act's provisions were partial and enforcement lagged; and the new DPDP Act, while a significant step, includes broad exemptions and insufficient checks on executive power.

In practice, Indian citizens frequently surrender their biometric data without knowing how it will be used or kept secure. Government agencies enjoy a wide array of immunities to deploy advanced surveillance under the guise of security, as seen in the Criminal Procedure amendments and FRT projects, with limited legal oversight.

Corporations, too, find ways to harness biometrics (for user convenience, targeted services, or national security contracts) in a mostly unregulated sea of data. When breaches occur – as with Aadhaar leaks or police database hacks – the affected individuals have almost no remedy under Indian law, aside from filing police complaints or seeking limited relief in court.

Looking forward, there remain grey zones and open to a wide spectrum of unexpected curiosities. How will India's judiciary respond when FRT's constitutionality is fully tested? Will the Data Protection Board evolve into an independent regulator? Can the DPDP Act's provisions be tightened through rules or judicial interpretation to better safeguard consent and transparency? Or will the status quo persist, effectively exempting state actors from privacy norms? The answers will shape whether India's privacy jurisprudence merely echoes the Puttaswamy ideals, or falls short in practice. Internationally, India is far from alone in confronting these dilemmas. While the EU and some U.S. states have taken stricter stances, many countries are grappling with the trade-offs. But India's unique social and administrative context –

[81] *California Consumer Privacy Act (CCPA)*, State of California - Department of Justice - Office of the Attorney General (Oct. 15, 2018), https://oag.ca.gov/privacy/ccpa.

[82] *The American Privacy Rights Act | Congress.Gov | Library of Congress*, https://www.congress.gov/crs-product/LSB11161 (last visited May 11, 2025).

its massive population, digital identity infrastructure, and ambitious surveillance programs – means the stakes may be higher. To borrow an insight from observers of global biometric systems, it is not enough to deploy these technologies; "much, much more is durably required" in terms of legal and institutional safeguards.[83] Whether India meets this requirement remains to be seen.

[83] 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).