AADHAR AND THE ARCHITECTURE OF CONSENT: PROTECTING THE WORLD'S LARGEST BIOMETRIC DATABASE

Rohan Bhimajiyani, LL.M., Gujarat National Law University

ABSTRACT

With the rise of digitalisation in every realm of our lives, governments around the world have embraced technology to deliver welfare services to their citizens. It provides a secure, cost-effective and modern solution to the legacy methods of service delivery.

The Government of India has undertaken the 'Digital India' project under which various services have been made digital. The government has leveraged technology to deliver services to the masses and build lasting infrastructure, which it calls 'Digital Public Infrastructure' to be used as public goods. The JAM Trinity, as it is colloquially known, consists of Jan Dhan, Aadhar and Mobile numbers. It consists of complete private information of a citizen, which is used to deliver services. Aadhar was started as a way to streamline benefit delivery to the marginalised. However, over the years, it has developed into a prerequisite for accessing any government service, making it challenging to opt out by design, putting in question the consent of citizens.

The Supreme Court of India in the KS Puttaswamy v. Union of India recognised the fundamental right to privacy under Article 21 of the Constitution; the Digital Personal Data Protection Act 2023 provides for the protection of the data of citizens. This paper aims to explore the privacy risks associated with the rise of Aadhaar and other such technologies. The authors look into the progression of Aadhar over the years and the existing legal framework around data protection. We then compare global best practices to analyse how India can ensure it protects the largest biometric database in the world. We end the paper with our suggestions and the way forward.

Introduction

India's ambitious digital identity programme, Aadhaar, has become the world's largest biometric database used by over 1.3 billion people.[1] Conceived as a base identity system, Aadhaar captures and stores distinctive biometric and demographic-related data (fingerprints, iris scans and other sensitive information) -- to authenticate for an extensive range of services provided by the government as well as by the private sector, including banking, welfare benefits, taxation, and telecommunication. It was a vision of an integrated digital backbone that would encourage inclusivity, transparency and efficiency in service delivery. But with the growing reach of Aadhaar, issues of consent, privacy[2] and personal autonomy have now assumed the centre stage in Indian legal, ethical, and socio-political conversations.[3]

The objective of this paper is to analyse Aadhaar and the architecture of consent with a critical scrutiny. It focuses, in particular, on how consent is conceptualised, elicited and given effect to in the Aadhaar system and whether consent is indeed voluntary, informed and meaningful in practice. The paper examines whether the current data protection and privacy regime is adequate to protect the dignity of individuals from possible misuse of biometrics in India. It also locates Aadhaar in the worldwide discussions on digital identity, focusing on both its innovative history and potential threats to democratic freedoms. In this, the paper suggests that Aadhaar, while technically sound, is in danger of being constitutionally perverse unless it is rooted in a stronger foundation of consent and privacy and holds up to accountability.

The Evolution of Human Rights: From Three Generations to the Emerging Fourth

Human rights have evolved through distinct phases, each responding to the changing needs and challenges of human society.[4] The traditional framework recognizes three generations of rights, with a fourth generation now emerging in response to technological advancement and contemporary ethical concerns.[5]

---

[1] *Government of India taking measures to enhance the reach of Indian Digital Public Infrastructure*. Available at: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2037598 (Accessed: 30 August 2025).
[2] Saurav Kumar, *PRIVACY WITH RESPECT TO AADHAR IN RECENT DEVELOPMENTS*.
[3] 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).
[4] *Three generations of human rights*. Available at: https://lawpunditsglobal.com/media/uploads/2014/03/Three-Generations-Of-Human-Rights1.pdf (Accessed: 30 August 2025).
[5] Woodroofe, J.,*A fourth generation of human rights?*, *The Organization for World Peace*. Available at: https://theowp.org/a-fourth-generation-of-human-rights/ (Accessed: 30 August 2025).

The Three Established Generations

First Generation: Civil and Political Rights (18th Century): First-generation rights emerged from the liberal revolutions of the 17th and 18th centuries, particularly influenced by the French and American revolutions. These rights embody the principle of liberty and focus on protecting individual freedom from state interference

Second Generation: Economic, Social and Cultural Rights (19th Century): The second generation emerged during the 19th century industrial revolution. These rights embody the principle of equality and include positive rights that require active state intervention to ensure basic human needs are met.

Third Generation: Collective and Solidarity Rights (20th Century): Third-generation rights emerged in the latter half of the 20th century. These rights embody the principle of fraternity or solidarity and focus on collective rather than individual rights.[6]

The Emerging Fourth Generation of Human Rights

The fourth generation of human rights is currently developing in response to rapid technological advancement, biotechnology, and the digital transformation of society. This generation addresses new ethical and legal challenges that previous frameworks could not anticipate, particularly in the realms of digital technology and bioethics.[7]

Digital Rights

Fourth-generation digital rights recognize that technology has become integral to human life and that access to digital spaces is essential for exercising other fundamental rights. These rights include internet access, digital privacy, the right to be forgotten, protection from algorithmic discrimination, and digital identity rights. The United Nations Human Rights Council has recognized internet freedom as a human right, acknowledging that digital technologies can both enhance and threaten fundamental freedoms.[8]

---

[6] *Evolution and generations of human rights* (2025) *Blogs*. Available at: https://superkalam.com/upsc-mains/topics/evolution-three-generations-human-rights (Accessed: 30 August 2025).
[7] Olha O. Barabash et al., *The Fourth Generation of Human Rights: European Standards and National Experience*, BOL. MEX. DERECHO COMP. 3 (2024).
[8] *Article 12: The right to privacy*, *Digital Freedom Fund*. Available at: https://digitalfreedomfund.org/digital-rights-are-human-rights/article-12-the-right-to-privacy/ (Accessed: 30 August 2025).

Privacy as a Fourth-Generation Human Right in the Internet Age

Privacy in the digital age exemplifies fourth-generation human rights, as it addresses challenges that were inconceivable when earlier generations of rights were established. While privacy was recognized in Article 12 of the Universal Declaration of Human Rights in 1948, the internet era has fundamentally transformed both the nature of privacy threats and the scope of privacy protection needed.[9]

The Digital Privacy Challenge

Modern digital technologies enable unprecedented data collection, storage, and analysis capabilities that extend far beyond traditional privacy concerns. Every aspect of human life now generates digital footprints—location data, communications, purchases, searches, and health information—creating comprehensive profiles of individuals. Governments and private companies can engage in mass surveillance that would have been technically impossible in earlier eras.[10]

Privacy as an Enabling Right

Digital privacy serves as an enabling right that facilitates the exercise of other fundamental freedoms. Without privacy protection, individuals cannot freely express themselves, associate with others, or participate in democratic processes without fear of surveillance or discrimination.[11] Privacy enables authentic self-development by providing space for individuals to explore ideas, relationships, and identities without judgment.[12]

Legal Recognition and Protection

Recent legal developments have begun recognizing digital privacy as a fundamental human right. The European Union's General Data Protection Regulation (GDPR) and similar

[9] (No date a) *Human rights in the Digital age | OECD*. Available at: https://www.oecd.org/en/topics/sub-issues/human-rights-in-the-digital-age.html (Accessed: 30 August 2025).
[10] Hlophe, N. (2025) *Data Privacy in the digital era: Are human rights at risk?* , *Digital Frontiers Institute*. Available at: https://digitalfrontiersinstitute.org/data-privacy-in-the-digital-era-are-human-rights-at-risk/ (Accessed: 30 August 2025).
[11] *Privacy what it is and why it is important* : Available at: https://sherloc.unodc.org/cld/zh/education/tertiary/cybercrime/module-10/key-issues/privacy-what-it-is-and-why-it-is-important.html (Accessed: 30 August 2025).
[12] *Understanding data privacy as a human right*, *The Legal School: Law Courses for Legal Professionals & Students*. Available at: https://thelegalschool.in/blog/data-privacy-as-a-human-right (Accessed: 30 August 2025).

legislation worldwide establish comprehensive frameworks for protecting personal data. Courts, including India's Supreme Court in the Puttaswamy case[13], have explicitly recognized privacy as a fundamental right essential for human dignity in the digital age.[14]

The emergence of fourth-generation human rights, particularly digital privacy rights, reflects humanity's ongoing struggle to protect fundamental values in the face of technological change. As artificial intelligence[15], biotechnology, and digital surveillance capabilities continue advancing, the recognition and protection of these evolving rights will become increasingly crucial for maintaining human dignity and democratic society in the 21st century.

Aadhaar now serves as a test case for how societies grapple with trade-offs between the aspiration of technological opportunity and the preservation of basic freedoms.[16]

Aadhar: The Largest Biometric Database in the World

Historical Context and Evolution

Conceptually, a national identity system in India was not a novel idea when Aadhaar was rolled out in 2009. For years, the Indian state had struggled with the problems of identification, welfare targeting, and incorporating the poor and undocumented. Ration, voter (as in voter card), and PAN (Permanent Account Number) cards were commonly used but highly fragmented, duplicate-prone, and non-interoperable. This led to inefficiency, corruption, and wastage in the distribution of welfare.[17] From its inception as a voluntary programme, Aadhaar's mantra was financial inclusion and welfare rationalisation.[18] But it has since become an integral part of the machinery of the state, reaching into the realms of banking, taxation, the cell phone network, "live working", and education. By 2016, the Aadhaar (Targeted Delivery

[13] Justice K.S Puttaswamy (Retd.) v. Union of India, 2019 (1) SCC 1.
[14]Office of the Privacy Commissioner of Canada (2023) *Privacy as a fundamental right in the Digital age*, *Office of the Privacy Commissioner of Canada*. Available at: https://www.priv.gc.ca/en/opc-news/speeches-and-statements/2023/sp-d_20230224/ (Accessed: 30 August 2025).
[15] Gicj (2024) *GICJ*, *Geneva International Centre for Justice*. Available at: https://www.gicj.org/topics/thematic-issues/business-human-rights/3758-digital-rights-the-impact-of-ai-and-emerging-technologies-on-human-rights (Accessed: 30 August 2025).
[16] Janaki Srinivasan, *The Poverty of Privacy: Understanding Privacy Trade-Offs From Identity Infrastructure Users in India* (2018).
[17]TNN / Updated: Sep 27, 2018 (no date) *A brief history of the Unique Identity Project*, *The Times of India*. Available at: https://timesofindia.indiatimes.com/business/sc-holds-aadhaar-valid-a-brief-history-of-a-unique-identity-project/articleshow/65975093.cms (Accessed: 30 August 2025).
[18] Asha Gupta, *Digitalisation of the Welfare State: Lessons for the Emerging Economies*, 69 INDIAN JOURNAL OF PUBLIC ADMINISTRATION 453 (2023).

of Financial and Other Subsidies, Benefits and Services) Act[19] granted it statutory support, making it an indispensable lynchpin of India's digital governance model.[20] Aadhar now forms part of the digital public goods[21] as part of the India Stack.

The reach of Aadhaar is like no other:

- Direct Benefit Transfers (DBT): Subsidies for food, fuel, and welfare schemes are digitally transferred through the Aadhaar-seeding bank accounts, minimising leakages. There are claims of security and nearly ₹90,000 crore (approx $11 billion), the amount being saved annually by Aadhaar-based transfer, between 2014–2018.[22]

- Financial Inclusion: Aadhaar was the backbone of the Jan Dhan Yojana, which resulted in the opening of more than 500 million bank accounts, many of these with Aadhaar-based eKYC.[23]

- Connectivity: The telcos leverage Aadhaar for a KYC check to issue a SIM card quickly.

- Tax: PAN-Aadhaar linking is compulsory now to cut down on tax evasion.

Across the board, the fact that Aadhaar has penetrated everyday transactions, from being given rations, to withdrawing pensions, to filing tax returns—for good or ill—also speaks to its transformational potential. But it also throws up questions of dependence, exclusion, and privacy once Aadhaar validation is a failure or is abused.[24]

Aadhaar's design is based around "one person, one identity." This is made possible by enrolling

[19] The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (India).
[20] *The digital transformation and efficiency of India's direct benefit transfer model*. Available at: https://ddnews.gov.in/en/the-digital-transformation-and-efficiency-of-indias-direct-benefit-transfer-model-2/ (Accessed: 30 August 2025).
[21] Uttara Purandare, *Digital Infrastructure: Public Good or Private Commodity?—Rethinking the Right to Internet Access in the Context of Urban Digitisation*, 29 SCIENCE, TECHNOLOGY AND SOCIETY 555 (2024).
[22] *Direct benefit transfer – a blessing during the time of pandemic | national informatics centre | india*. Available at: https://www.nic.gov.in/blog/direct-benefit-transfer-a-blessing-during-the-time-of-pandemic/ (Accessed: 30 August 2025).
[23] *Direct benefit transfer initiative saved ₹3.48 lakh CR by reducing leakages: It minister*, *Newsonair*. Available at: https://www.newsonair.gov.in/direct-benefit-transfer-initiative-saved-%E2%82%B93-48-lakh-cr-by-reducing-leakages-it-minister/ (Accessed: 30 August 2025).
[24] Pawan Singh, *Aadhaar and Data Privacy: Biometric Identification and Anxieties of Recognition in India*, 24 INFORMATION, COMMUNICATION & SOCIETY 978 (2021).

the demographic and the biometric data at the enrolment phase.

1. Demographics: Name, Age, Sex, Residence, Mobile, E-mail.

2. Biometric Data:

- Ten fingerprints
- Two iris scans
- Facial photograph

This data is maintained in the Central Identities Data Repository (CIDR), a large, centralised database controlled by UIDAI.

Authentication Ecosystem

The power of Aadhaar is in its authentication services:

- Biometric Recognition: Comparing fingerprints or iris scans to the data.
- OTP: Sent to your registered mobile number.
- Demographic verification: Same demographic information submitted by citizens and existing in CIDR.

This multi-modal system makes Aadhaar a real-time identity verification system that can handle several billion transactions a year.

The Architecture of Consent in Aadhaar

The Aadhaar project is not only a technical architecture of biometric and demographic databases, but also a system of governance that rests on consent as a principle through which biometric data is collected and accessed. In theory, consent is supposed to protect individual autonomy and ensure that only the state and the private parties using Aadhaar use it for legitimate purposes. But the way in which this consent is implemented, construed, and imposed has been praised and criticised. We discuss the consent architecture in the Aadhaar system, within that ecosystem, by looking at the law, the process of authentication, the Court's

interventions, and the comparison between the use of Aadhaar in welfare systems and in the private sector.[25] Although the Aadhaar Act and judicial oversight want to entrench "informed consent" as the cornerstone of the system, in practice, things have been a lot messier. Consent in Aadhaar is not necessarily informed, voluntary, or meaningful, especially when you consider India's socioeconomic diversity, differential levels of digital literacy, and the power asymmetry between the state and the citizen.

Challenges in the Consent Framework of Aadhar:

Informed vs. Illusory Consent

It is a positive legal requirement that persons need to be told at the time of authentication of the nature of the information that is being employed for authentication, and how this will be used, as per the Aadhaar Act. Yet in reality, informed consent frequently devolves to consent in camouflage.

- Jargon: Our authentication forms, privacy notices, and consent screens are all written in a bureaucratic or technical legal voice that one could only hope that beneficiaries understand.
- Lack of information: A large number of people might be unaware of their biometric/ demographic data protection, data storage, its accessibility, and retention period.
- Authority Trust: Since state agencies hold significant power over the individual, quite often, beneficiaries will consent without challenge, trusting the state to make the best choice for them.

Therefore, consent often becomes a bureaucratic rubber-stamp rather than a substantial assertion of autonomy.

Digital Literacy Challenge

Digital consent presumes a basic literacy, as well as a familiarity with technology. But India's digital divide is a major obstacle:

[25] Amlegals (2024) *Data Privacy n the context of Aadhaar and India's Digital Identity Systems*, *Corporate Law Firm in Ahmedabad, India.* Available at: https://amlegals.com/data-privacy-in-the-context-of-aadhaar-and-indias-digital-identity-systems/# (Accessed: 30 August 2025).

- India has less than 40% of household Internet penetration, and, at best, one out of three Indians has a level of digital literacy. [26]

- A majority of residents cannot read consent messages on screens or comprehend technical aspects of, say, biometric authentication.

- It has been reported of instances where a person places a fingerprint on a reader without even knowing what they are consenting to do, turning consent into a blind transaction.

This is the death knell for informed consent, as the possibility to understand and weigh options is unavailable to large swaths of the population.

Coercion and Conditionality

The biggest problem is that consent in Aadhaar is seldom voluntary. Instead, it often becomes forced, particularly in welfare settings.

- Those who are beneficiaries of the Public Distribution System (PDS), pension schemes, LPG subsidies, or MNREGA wages are typically notified that they need to link Aadhaar or are made to authenticate through biometric recognition even to get their entitlements.

- Across states such as Jharkhand and Rajasthan, we have heard reports of people being denied rations or pensions based on failed Aadhaar validation, including the elderly, working women, and daily wage labourers.[27]

Therefore, what is described as consent is not real consent, and its validity, based on constitutional principles of autonomy and dignity, is dubious.

Use Expanding Function Creep and Use

Another important problem is 'function creep'[28] — or the stretching of the use of Aadhaar

[26] *Universal connectivity and Digital India initiatives reaching to all areas, including tier-2/3 cities and villages*. Available at: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2040566 (Accessed: 30 August 2025).
[27]Sardesai, S. (2021a) *When Aadhaar-related problems lead to denial of rations and benefits: What the data show*, *The Indian Express*. Available at: https://indianexpress.com/article/explained/explained-when-aadhaar-related-problems-lead-to-denial-of-rations-and-benefits-what-the-data-show-7277092/ (Accessed: 30 August 2025).
[28] *The wire: The Wire News India, Latest News,news from India, politics, External Affairs, science, economics, gender and culture.* Available at: https://thewire.in/politics/government/aadhaar-function-creep-uid (Accessed:

beyond its intended scope of targeted welfare delivery.[29]

- Conceived as a delivery vehicle for welfare and subsidies, Aadhaar rapidly expanded into SIM card verification, banking, property registration, and even school admissions.

- Although the Supreme Court restricted Aadhaar's use by the private sector, enabling it in financial companies and telecom service providers through cascading amendments and administrative decisions, it has reopened a can of worms of what Aadhaar can and cannot be used for.

- This growth weakens the foundation of purpose limitation —one of the building blocks of consent in a meaningful way. When citizens agree to use Aadhaar authentication for a particular purpose (e.g., PDS), the data input for that purpose is not likely to be reused by the system for entirely different purposes (e.g., credit profiling).

Function creep proliferates misuse and undermines the framework of trust that consent is supposed to provide in Aadhaar.

Security of Data: Risk of Breaches

The Aadhaar consent is also diluted by the lack of data protection and security. Even among people who are willing to turn over information, their trust that their privacy will be protected is inextricably linked to strong protections against breaches and abuse.

- There have been several incidents over the years where Aadhaar data has been leaked from government websites, disclosing the demographic information of millions of users.[30]

- In 2018, it was widely reported that Aadhaar numbers and details could be purchased by unauthorised people from dealers offering them for as little as ₹500.

---

30 August 2025).

[29]Mukhopadhyay, D. (2020b) *While India copes with covid-19, Aadhaar continues its function creep #saveourprivacy*, *Internet Freedom Foundation.* Available at: https://internetfreedom.in/aadhaar-good-governance-rules/#:~:text=The%20latest%20Aadhaar%20Good%20Governance,and%20the%20spread%20of%20knowledge (Accessed: 30 August 2025).

[30] Et *Data breach: Aadhaar Data Leak: Personal Data of 81.5 crore Indians on sale on dark web: Report*, *The Economic Times*. Available at: https://economictimes.indiatimes.com/tech/technology/aadhar-data-leak-personal-data-of-81-5-crore-indians-on-sale-on-dark-web-report/articleshow/104856898.cms?from=mdr (Accessed: 30 August 2025).

- UIDAI maintains that the Central Identities Data Repository (CIDR) has never been breached, but a series of peripheral leaks demonstrates that an individual may not have control over her data even after she has given consent.

Without robust and enforceable data protection laws the Indian Digital Personal Data Protection Act, 2023, is a step in the right direction consent can become an empty concept in the face of systemic weaknesses.

Legal Framework

Legal Framework: Aadhaar Act 2016 and Amendments

Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, is the law that gives this Act its teeth. The biometric (fingerprints, iris scans, and facial photo) and demographic data of individuals who join the system are retained in the Central Identities Data Repository (CIDR) of Unique Identification Authority of India (UIDAI), comprises of the UIDAI (Terms and Conditions of Service of Chairperson and Members) Rules, 2009.

Section 8 of the Act explains the method of consent. It states that:

Aadhaar number holders are required to give their consent before any entity can use their identity information for authentication.

Identity authentication entities should prompt individuals to know the kind of their registered information, the purpose of the authentication, and the goings-on involved by the parties concerned.

Consent has to be “informed”, which means that the Aadhaar holder knows and consents to the use of the information for the stated purpose.

The amended laws in 2019 and 2021 sought to further crystallise the uses of Aadhaar, particularly after the Supreme Court intervened in the Puttaswamy judgment. These changes clarified that Aadhaar could be applied for government subsidies and select regulation-compliant private use cases (banking, telecom), but that in other contexts, its usage must be voluntary.

How Authentication and Consent Mechanisms Work in the Real World

Technically, while online authentication of Aadhaar works on the real-time matching (either biometric or demographic) of the data with the CIDR, in offline authentication, a successful offline verification can be done at the service provider's end. When someone provides an Aadhaar number, the authentication agency seeks permission for authenticating the information, he had said. This approval can be in digital form (for example, by biometric scan prompt or OTP validation).

There are multiple authentication types:

Demographic verification – confirming the individual is who they claim to be.

OTP – (One Time Password) Authentication by authorising using the OTP received on the registered mobile number.

Biometric Authentication -The fingerprints or iris scans are used to provide consent as well as verify.

Although UIDAI norms categorically stipulate that the purpose behind collecting an individual's data in the authentication process has to be divulged to the individual, the principle of 'informed consent' does not really work in the true spirit. Many people, especially in rural areas or those with low online literacy, have no idea what happens to their data or where it is stored. Rather, consent tends to be presumed by participating in schemes that require Aadhaar authentication for access.

The Puttaswamy Judgment & Right to Privacy

In the historic judgment of Justice K.S. Puttaswamy (Retd.) vs. Union of India[31] case reinvented the constitutional architecture of consent was reinvented in the context of Aadhaar. The Supreme Court held that: Privacy is a Fundamental Right under Article 21 of the Constitution. Aadhaar is constitutionally valid, but it is upon safeguards to prevent consent and function creep. Aadhaar cannot be compulsory for private services like telecom connections or school admissions.

[31] Justice K.S Puttaswamy (Retd.) v. Union of India, 2019 (1) SCC 1.

Aadhaar may be used for welfare subsidies where state interest is comparatively more than privacy risks, and consent is taken, and there is also a balancing through proportionality.

Among the most contested aspects of Aadhaar's consent architecture is the uneven treatment of consent in welfare and private sector points of access.

1. Welfare Schemes

Aadhaar has been adopted for schemes such as the Public Distribution System (PDS), MNREGA, LPG subsidies, and pension schemes. In theory, beneficiaries must have consented to Aadhaar authentication. But assuming that consent can in fact be obtained, in practice, it's coercive consent because the alternative seems to be starving or distressing without benefits. For the marginalised, there is no bright line between voluntary and coerced consent.

2. Private Sector Applications

Before the Supreme Court order, Aadhaar was widely used by telecom companies, as well as banks and financial technology companies, for e-KYC incentives. Here, the consent was nominally voluntary but in practice coerced consumers frequently had no option but to submit their Aadhaar. After the Puttaswamy judgment, private sector use of Aadhaar has been limited, but there are exceptions where Aadhaar may be used under statutory regimes.

DPDP Act

India's evolving data protection landscape, culminating in the Digital Personal Data Protection Act 2023,[32] marks significant progress but leaves critical gaps in biometric data governance. The DPDPA establishes consent-based processing requirements and individual rights frameworks, yet it lacks specific provisions for the unique challenges posed by biometric identifiers.[33] The absence of clear data minimization standards, limited right to erasure for biometric data, and insufficient cross-border transfer restrictions create regulatory vulnerabilities.[34] The Aadhar Act itself predates comprehensive privacy legislation and

[32] Anirudh Burman, *Understanding India's new Data Protection Law*, *Carnegie Endowment for International Peace*. Available at: https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en (Accessed: 30 August 2025).
[33] Srinivas Katkuri, *Need of Encryption Legislation: Protecting India's Digital Realm and Beyond*, 70 INDIAN JOURNAL OF PUBLIC ADMINISTRATION 562 (2024).
[34] *Comply with DPDPA and Aadhaar as one | india | law.asia*. Available at: https://law.asia/aadhaar-dpdpa-compliance/ (Accessed: 30 August 2025).

contains limited privacy safeguards compared to international standards.[35] While the Supreme Court's 2018 ruling restricted mandatory Aadhar usage in certain contexts, the system's extensive integration across public and private sectors continues to expand without proportionate privacy protections. This regulatory lag between technological deployment and legal protection represents a fundamental governance challenge requiring immediate attention

DPDP Act Provisions for Aadhaar and Biometric Data Protection

The Digital Personal Data Protection Act 2023 (DPDP Act)[36] establishes a comprehensive framework for protecting biometric data within India's Aadhaar ecosystem, emphasizing four key principles: consent, purpose limitation, data minimization, and accountability.[37]

Core Protection Mechanisms

Consent Requirements: The DPDP Act mandates that biometric data can only be collected for legitimate purposes critical to the data fiduciary's function. Organizations must obtain explicit, informed, and verifiable consent from individuals before collecting biometric data, accompanied by clear notices specifying all data principal rights and grievance redressal mechanisms. For children under 18, parental consent is mandatory.[38]

Purpose Limitation and Data Minimization: Biometric data collection is strictly subject to purpose limitation - organizations can only collect what is necessary for specified purposes and must delete the data once that purpose is fulfilled. The Act prohibits using biometric data for reasons other than compelling legitimate uses, addressing concerns about mass surveillance and unauthorized profiling.[39]

---

[35] Rukmini Bhattacharjee, *Data Protection for Democratic E-Governance in India*, 70 INDIAN JOURNAL OF PUBLIC ADMINISTRATION 631 (2024).

[36] *The Digital Personal Data Protection Act, 2023 ...* Available at: https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf (Accessed: 30 August 2025).

[37] Rana, A. (2025) *Understanding the aadhaar (sharing of information) amendment regulations, 2025*, *Data Protection - India*. Available at: https://www.mondaq.com/india/data-protection/1670376/understanding-the-aadhaar-sharing-of-information-amendment-regulations-2025 (Accessed: 30 August 2025).

[38] *Regulation of biometric data under the DPDP Act* (2023) *King Stubb & Kasiva*. Available at: https://ksandk.com/data-protection-and-data-privacy/regulation-of-biometric-data-under-the-dpdp-act/ (Accessed: 30 August 2025).

[39] *Biometric data regulation in India: Legal landscape and risks* (no date) *azb*. Available at: https://www.azbpartners.com/bank/biometric-data-regulation-in-india-legal-landscape-and-risks (Accessed: 30 August 2025).

Aadhaar-Specific Compliance

Storage and Retention Restrictions: Under the DPDP framework, Aadhaar numbers and biometric data cannot be stored or retained without explicit permission. Organizations must implement data masking, displaying only the last four digits of Aadhaar numbers by default, with full numbers visible only on a "need to know" basis. Transaction logs are automatically deleted after six months to prevent long-term tracking.

Security Standards: The Act requires robust security protocols including mandatory encryption for data storage and transmission, access controls, and the use of only STQC-certified biometric devices for authentication. Organizations must report security incidents affecting Aadhaar data to UIDAI immediately and implement appropriate confidentiality obligations through non-disclosure agreements.

Enhanced Protection Framework

Data Principal Rights: The DPDP Act grants individuals comprehensive rights over their biometric data, including access to information about data processing, correction of inaccuracies, and erasure rights once the processing purpose is fulfilled. Individuals can withdraw consent at any time, requiring organizations to cease processing and delete the data.

Organizational Obligations: Data fiduciaries handling biometric data must appoint Data Protection Officers and implement consent management systems. The Act establishes heavy penalties up to ₹250 crores for non-compliance, creating strong incentives for proper data protection.

Limitations and Gaps

While the DPDP Act significantly enhances biometric data protection, it does not categorize biometric data as sensitive personal data requiring special protection, unlike international frameworks such as GDPR. The Act also provides "legitimate use" exemptions for state functions, which could potentially allow government agencies broader access to biometric data without explicit consent.

The framework represents a substantial improvement over previous regulations, with UIDAI

asserting that Aadhaar operations exceed DPDP requirements in several areas.[40] However, effective implementation depends on forthcoming rules and the establishment of the Data Protection Board of India to oversee compliance and enforcement.

Global Best Practices in Data Protection

Global Biometric Data Protection Frameworks

Jurisdiction	Primary Law	Classification	Key Requirements	Consent Requirements	Enforcement
European Union	GDPR (2018)	Special Category Data	Purpose limitation, data minimization, privacy by design	Explicit consent required	Up to €20M or 4% annual turnover
US (Illinois)	BIPA (2008)	Biometric Identifiers	Written consent, disclosure of purpose & duration	Written consent mandatory	$1k–
US (California)	CCPA (2020)	Personal Information	Right to know, delete, opt-out of sale	Opt-in for sensitive data under 16	Up to $7.5k per violation
China	PIPL (2021)	Sensitive Personal Info	Specific purpose, necessity demonstration	Explicit consent for sensitive data	Up to RMB 50M or 5% revenue
India	Aadhaar & DPDP Act	Sensitive Personal Data	Purpose limitation, data localization	Explicit consent required	Penalties up to INR 250 crores
Canada	PIPEDA	Highly Sensitive Info	Express consent, necessity principle	Express informed consent	Federal Privacy Commissioner
Australia	Privacy Act 1988	Sensitive Information	Consent or legal authorization	Consent required unless exception	Civil penalty up to AUD 2.2M
Singapore	PDPA	Personal Data	Consent, purpose limitation, security	Consent required with exceptions	Financial penalties up to SGD 1M
Brazil	LGPD (2020)	Sensitive Personal Data	Specific consent, data minimization	Specific and distinct consent	Up to 2% revenue or BRL 50M
South Africa	POPIA (2021)	Special Personal Info	Prior authorization for processing	Voluntary, specific, informed	Information Regulator oversight

European Union: The GDPR Gold Standard

The European Union's General Data Protection Regulation (GDPR) sets the global benchmark for biometric data protection,[41] classifying biometric data as "special category data" requiring enhanced protection. Key GDPR principles include[42]:

Explicit Consent Requirements: Organizations must obtain explicit, informed consent before

[40]Gupta, O. (2025) *The financial express*, *India News | The Financial Express*. Available at: https://www.financialexpress.com/india-news/aadhaar-fully-complies-with-data-protection-law-uidai-chief/3935814/ (Accessed: 30 August 2025).
[41] Sahoo, N. (2025) *Privacy implications for GDPR & biometric data*, *Information Security Consulting Company - VISTA InfoSec*. Available at: https://vistainfosec.com/blog/gdpr-biometric-data-ethical-privacy/ (Accessed: 30 August 2025).
[42] *Biometric data GDPR: Compliance tips for businesses* (2025) *GDPR Register | Compliance Software Tools for Privacy Teams*. Available at: https://www.gdprregister.eu/gdpr/biometric-data-gdpr/ (Accessed: 30 August 2025).

processing biometric data, with the data subject fully understanding the collection purpose and usage.

Data Minimization Principle: Only the minimum amount of biometric data necessary for the stated purpose should be collected.

Privacy by Design: Data protection must be integrated into system design from the outset, avoiding "function creep" where data is used beyond its original purpose.

Right to Erasure: Individuals maintain the right to have their biometric data deleted when it is no longer necessary.

GDPR's consent requirements mandate that individuals receive clear, granular information about data processing purposes and can withdraw consent at any time. The regulation's breach notification requirements - notification to authorities within 72 hours and affected individuals without undue delay - establish accountability standards that exceed current Indian frameworks. Financial penalties reaching 4% of global turnover create meaningful enforcement mechanisms that ensure compliance. The regulation's emphasis on data minimization - collecting only necessary data for specified purposes - directly addresses one of Aadhar's core vulnerabilities: the extensive collection and retention of biometric identifiers without clear purpose limitations. GDPR's approach to international data transfers, requiring adequacy decisions or appropriate safeguards, offers a model for protecting Indian citizens' data from unauthorized foreign access.

Estonia's Distributed Digital Identity Model

Estonia's digital identity system demonstrates how national-scale identity infrastructure can operate with enhanced privacy protections through distributed architecture and transparent governance. Unlike Aadhar's centralized model, Estonia employs X-Road technology that enables secure data sharing between agencies without creating a single point of vulnerability. Citizens maintain control through access logs and data tracker tools that show exactly who accessed their information and when.[43]

The Estonian system incorporates several privacy-enhancing features absent from Aadhar:

[43] *Definitions in Estonia - Data Protection Laws of the World*. Available at: https://www.dlapiperdataprotection.com/?t=definitions&c=EE#insight (Accessed: 30 August 2025).

distributed database architecture prevents single-point failures, mandatory access logging creates accountability trails, and citizens receive notifications for all data access attempts. The system's transparency extends to public availability of security measures and regular independent audits. Despite handling sensitive government services including voting and healthcare, Estonia has maintained public trust through consistent transparency and user control mechanisms.[44]

Estonia's legal framework integrates constitutional privacy protections with operational requirements, creating clear boundaries for data use. The system's 20-year operational history provides evidence that sophisticated digital identity infrastructure can operate at national scale while preserving individual privacy rights. This experience offers valuable lessons for reforming Aadhar's architecture to better balance functionality with privacy protection.[45]

United States: State-Level Innovation

Illinois Biometric Information Privacy Act (BIPA): As the most stringent biometric privacy law in the United States, BIPA requires companies to obtain written consent before collecting biometric data, inform individuals of the specific purpose and duration of data collection, and provide a private right of action for violations.

Key BIPA Requirements:

- Written consent for each biometric identifier collection
- Disclosure of purpose and retention period
- Secure storage requirements
- Statutory damages of $1,000-$5,000 per violation

Suggestions and Recommendations

1. Establish Third Party Security Auditors: The Government must establish a third-party

[44] *Data Protected Estonia: Insights* (no date) *Linklaters*. Available at: https://www.linklaters.com/en/insights/data-protected/data-protected---estonia (Accessed: 30 August 2025).
[45] Hubner, R. (2021) *Spotlight: How are data protection laws enforced in Estonia?*, *Lexology*. Available at: https://www.lexology.com/library/detail.aspx?g=3b3316dd-e8ac-42dd-adc7-f3f580f94857 (Accessed: 30 August 2025).

auditor that will audit the safety practices and security infrastructure of UIDAI. This body shall conduct regular security audits to ensure continued data integrity of the Aadhar database. With the increasing amount of data collected by the program and the interlinkages with various government schemes, the risk of data profiling and consequences of data breach would be immense. The third-party body free from the control of the government or UIDAI is necessary to ensure data protection. This body can also look into upgrading the current infrastructure to ensure that security is enhanced. This can include upgrading the cryptographic algorithms deployed, server infrastructure and formulating SOPs in line with the global standards.

2. Citizen Centric Approach: The UIDAI should develop a more citizen centric approach when it comes to handling data of citizens. Providing more control of the data back to the citizens. Data minimization principles must be strictly enforced through technical and policy measures. UIDAI should implement purpose-specific data collection limits, automatic data deletion after specified retention periods, and granular consent mechanisms allowing individuals to control how their data is used. Regular privacy impact assessments should evaluate whether biometric authentication is necessary for each use case or whether less intrusive alternatives could achieve the same objectives.

   Another facet of a citizen centric approach includes the process of plugging information disparities in the system. No poor or marginalized person should be left out of the social security net either because he does not have an Aadhar card or because the database does not match with his details or failure of biometric authentication etc.

3. Strengthening the Legal Framework: Right to Privacy is already recognized under the Indian Constitution as part of Article 21. With the enactment of DPDP act, the legal framework of Data Protection has certainly improved. The acts governing Aadhar also have separate provisions for data protection. However with the increasing use of Aadhar by both Government and Private sector, increased protection is required. With know instances of data breach and function creep the government must work to restore data integrity and confidence of the public. The Government must look into the global best practices and implement them at the earliest, they can be modified according to the Indian context however we must strive for the ideal. With the government relying on Digital India and collecting more data than ever before, strict data protection regime must be put into place.

This will ensure that the citizens have confidence that their data is in good hands and is being protected from nefarious use. This will lead to faster adoption of various Digital India initiatives.

4. Enhancing the Consent Infrastructure: The Aadhar framework must work to get back to its origin in terms of consent. Over the years it has taken the form of a compulsion significantly reducing the scope of consent. With it being tied to accessing various government scheme benefits and the mandatory linking orders for things like PAN cards, mobile numbers, DEMAT accounts etc, reduce the scope of free consent. The following reforms are suggested in this regard,

   1. Awareness and Literacy: Citizens, especially those in the rural and local communities, require specific campaigns that educate them on their rights under Aadhaar. This also involves the knowledge of Virtual ID, Authentication History, and Data Portability.

   2. Consent Standardisation: Consents should be standard: simple, understandable, and free of technical gibberish, meaning just one consent to be given where everyone understands the meaning of it. All Aadhaar-enabled transactions should carry detailed information on the purpose of each transaction, its value and duration, as well as potential data-sharing.

   3. Revocability: Individuals must be able to withdraw their consent anytime, and it must be backed by user-friendly dashboards and redressal mechanisms.

5. Role of Civil Society Organizations: Civil Society actors like the Internet Freedom Foundation and global organizations like Freedom House conduct research on freedoms on the internet and conduct privacy advocacy for everyone. Such organizations must be supported and the recommendations given by such reports must be taken seriously. The government can include them as stakeholders while reworking the data protection laws and try to make stronger privacy laws. Civil Society actors can also conduct digital literacy drives. Such drives in partnership with the government can result in increased digital literacy around the frameworks of consent, digital rights available to the citizens, their right to privacy and the recourses available to them in case of privacy breach. Such measures will go a long way in encouraging the digital dignity of all.

Conclusion

In its promises and perils for technology, governance, and rights, as a biometric-based programme, the Aadhaar project perfectly approximates this intersection. The world's largest such registry, Aadhaar, is not just an administrative tool, but a marker of India's aspiration to re-imagine welfare delivery, access to finance, and state–citizen engagement in the digital era. But its vastness also amplifies the difficulties of privacy, consent, and accountability around experimentation — challenges that turn it into a test case for the entire world. Without informed and revocable consent, the Aadhaar would transform from a tool of empowerment to one of coercion. At the same time, there is no doubt that Aadhaar has revolutionised governance. There has been a reduction in subsidy leakages, millions have been brought into the fold of formal banking, and delivery processes have become much more efficient. In a country as large and heterogeneous as India, no reform on such a scale is without some blemishes. The balance that needs to be struck, however, is between the benefits of Aadhaar and the harm that can result from poor supervision, poor security, and digital exclusion. Those who are digitally illiterate or marginalised are at greatest risk of being exploited or excluded from the digital system, establishing the critical nature of creating inclusive policy. We look into the historical development of Aadhar and the various challenges it faces at the moment. The international best practices of Europe, USA, Estonia are reviewed to strengthen our own data protection regime. We conclude the paper with various recommendations including the establishment of an independent oversight authority to prevent misuse of data and ensure enhanced security. To promote a more citizen centric approach in handling the data and encouraging digital literacy which will ultimately improve the consent architecture. We are certain that with these recommendations implemented India can truly achieve the dream of being a digital and developed country.