INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

RIGHT TO PRIVACY AND AADHAAR-BASED BIOMETRIC SURVEILLANCE IN INDIA

AUTHORED BY - MAZHER ALI SIDDIQUI & DR ARVIND KUMAR SINGH
Amity University Lucknow

Abstract

The Aadhaar system, introduced in India as a biometric-based identity infrastructure, has fundamentally transformed the relationship between the Indian state and its citizens. By collecting fingerprints, iris scans, and demographic data of over a billion individuals, Aadhaar created what is arguably the world's largest biometric database. While its proponents argue that the system enables efficient delivery of welfare benefits, reduces corruption, and streamlines public administration, its critics have raised serious constitutional concerns about its compatibility with the fundamental right to privacy under Article 21 of the Constitution of India.

The Supreme Court of India, in the landmark judgment of K.S. Puttaswamy v. Union of India (2017), unanimously held that privacy is a fundamental right. This decision set the stage for a larger constitutional challenge to Aadhaar, which culminated in the five-judge bench decision in K.S. Puttaswamy v. Union of India (Aadhaar case) in 2018. While the Court upheld the core validity of Aadhaar, it also struck down several provisions and imposed significant restrictions on its use. Despite this, legal ambiguities remain, and the architecture of biometric surveillance continues to expand through interconnected databases, mandatory linkages, and increasing digitisation of government services.

This paper examines the constitutional dimensions of Aadhaar-based biometric surveillance in India. It analyses the right to privacy under Article 21, the architecture of the Aadhaar system, the judicial treatment of Aadhaar, and the continuing threats that biometric surveillance poses to fundamental rights. Drawing on comparative insights from international frameworks, the paper argues that India requires a comprehensive, rights-based legal framework to govern biometric data, prevent surveillance overreach, and uphold the constitutional promise of dignity and liberty.

ISSN: 2582-6433

Keywords: Right to Privacy, Article 21, Aadhaar, Biometric Surveillance, K.S. Puttaswamy, Fundamental Rights, Data Protection, Informational Privacy, Surveillance State, Constitutional Law, Digital Identity, Proportionality

Chapter 1: Introduction

1.1 Background

In an era defined by rapid technological expansion, the Indian state has increasingly turned to digital infrastructure to govern its vast and diverse population. The Aadhaar project, launched by the Unique Identification Authority of India (UIDAI) in 2009, stands as one of the most ambitious biometric identification programmes in the world. It assigns every resident a twelve- digit unique identification number backed by biometric data — fingerprints and iris scans — along with demographic details. As of 2024, over 1.3 billion Aadhaar numbers have been issued, making it the most extensive biometric database on the planet.

The stated purpose behind Aadhaar was pragmatic and welfare-oriented. The government sought to eliminate ghost beneficiaries from welfare schemes, reduce leakages in the public distribution system, and create a reliable method of authenticating identity in a country where documentary proof of identity was often unavailable to marginalised communities. On paper, Aadhaar offered the promise of inclusion. In practice, however, it raised a far more fundamental and troubling question: can the state compel its citizens to surrender their biometric identity as a condition for accessing rights, entitlements, and services?

1.2 The Constitutional Question

The constitutional significance of Aadhaar cannot be overstated. Article 21 of the Indian Constitution guarantees that no person shall be deprived of life or personal liberty except according to procedure established by law. Over decades of judicial interpretation, this deceptively brief provision has come to encompass a wide array of rights, including the right to dignity, the right to livelihood, and most recently, the right to privacy. The compulsory collection of biometric data, the construction of a central repository of such data, and the mandatory linkage of Aadhaar with bank accounts, mobile phones, and government services together form a surveillance architecture that directly engages with these constitutionally protected interests.

The right to privacy, finally and unambiguously recognised as a fundamental right by a nine-judge constitutional bench in 2017, forms the constitutional core of this discussion. The

ISSN: 2582-6433

question that this paper seeks to address is whether the Aadhaar-based biometric surveillance framework, as structured and implemented by the Indian state, is compatible with the constitutional guarantee of privacy under Article 21.

1.3 Scope and Objectives of the Study

This paper examines the constitutional, legal, and human rights dimensions of Aadhaar-based biometric surveillance. Its objectives are to trace the development of the right to privacy under Article 21; to examine the structural design, legislative framework, and administrative operation of the Aadhaar system; to analyse the constitutional challenges that biometric surveillance poses to fundamental rights including privacy, dignity, and the right against self-incrimination; to study the Supreme Court's treatment of these issues in the Puttaswamy litigation; to survey comparative approaches to biometric identity and data protection in other jurisdictions; and to recommend legal and institutional reforms necessary to bring India's biometric governance framework into harmony with constitutional values.

1.4 Research Methodology

This study adopts a doctrinal research methodology. It relies primarily on constitutional provisions, statutory texts, judicial decisions, law commission reports, and academic literature. Comparative analysis of foreign legal systems is used to contextualise and supplement the Indian experience. The paper also draws on reports by civil society organisations and policy bodies. A small-scale empirical survey has been incorporated in Chapter 9 to reflect ground-level awareness and concerns among students and academicians.

Chapter 2: The Right to Privacy Under Article 21

2.1 The Text and Early Interpretation of Article 21

Article 21 of the Constitution of India provides that no person shall be deprived of his life or personal liberty except according to procedure established by law.1 At the time of the Constitution's framing, the Constituent Assembly consciously chose the formulation 'procedure established by law' over the American formulation of 'due process of law.' This choice was interpreted, in the early post-independence years, to mean that the courts would not question the fairness or reasonableness of a legislative procedure as long as it was authorised by valid law. The Supreme Court in A.K. Gopalan v. State of Madras (1950) endorsed this narrow reading, confining Article 21 to procedural formalities.2

ISSN: 2582-6433

2.2 Maneka Gandhi and the Transformation of Article 21

The constitutional landscape changed decisively with Maneka Gandhi v. Union of India (1978), where a seven-judge bench of the Supreme Court overruled the restrictive interpretation of Gopalan.3 The Court held that the procedure established by law must itself be fair, just, and reasonable. An arbitrary or oppressive procedure would violate Article 21 even if sanctioned by a statute. This judgment introduced the idea of substantive due process into Indian constitutional law, and it laid the groundwork for the expansive jurisprudence that followed. From this point, the Court began reading into Article 21 a growing catalogue of rights beyond mere freedom from physical detention.

2.3 Privacy as a Constitutional Right: The Long Road

The recognition of privacy as a fundamental right did not come easily or immediately. For decades, the Supreme Court spoke of privacy in ambiguous terms. The Court in Kharak Singh v. State of Uttar Pradesh (1963) was divided on whether privacy was a constitutionally protected interest.4 A majority held that domiciliary visits by police violated Article 21, but the Court did not clearly articulate a general right to privacy. In Gobind v. State of Madhya Pradesh (1975), the Court acknowledged that privacy interests deserved constitutional protection but treated the right as subordinate to other pressing social interests.5 The position remained unsettled for decades.

2.4 K.S. Puttaswamy v. Union of India (2017): The Privacy Judgment

The matter was conclusively settled by the nine-judge constitutional bench in K.S. Puttaswamy v. Union of India (2017), popularly known as the Privacy Judgment.6 All nine judges unanimously held that the right to privacy is a fundamental right protected under the Constitution of India, drawing its existence from Articles 14, 19, and 21. Justice D.Y. Chandrachud, writing a concurring opinion, articulated a rich and multi-dimensional conception of privacy: privacy of the body, of personal choices, of informational autonomy, of communications, of location, and of identity.

Informational privacy — the right of individuals to control data about themselves — was identified as a core component of the right to privacy. The Court recognised that the digital age had created new threats to informational autonomy, and that the state must not collect, store, process, or disclose personal data without legal authority and proportionate justification. The judgment explicitly acknowledged that data about a person, especially sensitive data such as biometrics, is an extension of the person's identity and cannot be

ISSN: 2582-6433

appropriated by the state without constitutional justification.

2.5 The Proportionality Standard

The Privacy Judgment established that any state action restricting privacy must satisfy a four-part proportionality test: there must be a legitimate state aim; the means adopted must be rationally connected to that aim; the means must be necessary, meaning no less restrictive alternative must be available; and the measures must be proportionate to the rights violated in a broader balance of interests.7 This proportionality framework became the primary constitutional standard against which the Aadhaar framework would subsequently be tested.

2.6 Privacy, Dignity, and the Constitutional Core

The Privacy Judgment was equally emphatic that privacy is not merely an individual interest but is indispensable to human dignity. Dignity is the constitutional bedrock upon which the edifice of rights rests. A state that compels its citizens to reveal their most intimate biological characteristics — their fingerprints and iris patterns — as a precondition for accessing food, education, or healthcare, risks reducing the individual from a subject of rights to an object of administrative management. This tension between the state's interest in identification and the individual's interest in autonomy over her own body and data is the constitutional fault line on which the Aadhaar debate rests.

Chapter 3: Aadhaar – Architecture, Purpose, and Reach

3.1 Origins and Institutional Structure

The idea of a unique identification system for Indian residents was first proposed in 2006 through a report of the Planning Commission. The Unique Identification Authority of India (UIDAI) was established in 2009 under a Government of India notification, initially without any parliamentary authorisation. The UIDAI began enrolling residents and issuing Aadhaar numbers, collecting fingerprints, iris scans, and demographic information on a mass scale. The legal basis for this exercise was subsequently provided by the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, which was passed as a Money Bill — a procedural choice that would itself become a subject of significant constitutional controversy.8

ISSN: 2582-6433

3.2 The Biometric Architecture

At its core, Aadhaar is a biometric database. Every individual enrolled in the system provides ten fingerprints and two iris scans, which are stored in a centralised database maintained by the UIDAI. Authentication under the Aadhaar system works by matching the biometric data provided at the point of service with the data stored in the central repository. This creates a system where every authentication — every time an individual uses Aadhaar to access a service — generates a record in the central server. Over time, these records create a detailed log of an individual's interactions with the state and with private service providers.

3.3 The Scope of Mandatory Linkages

The initial voluntary nature of Aadhaar enrolment was progressively eroded through a series of government notifications and court orders. By 2017–18, Aadhaar had been made effectively mandatory for a vast range of purposes including filing income tax returns, obtaining PAN cards, opening bank accounts, obtaining mobile phone connections, accessing subsidies under virtually every welfare scheme, school admissions under mid-day meal programmes, and receiving salaries. The web of mandatory linkages created a situation where opting out of Aadhaar was, for practical purposes, equivalent to exclusion from civic and economic life.9

3.4 The Role of the Aadhaar Act, 2016

The Aadhaar Act, 2016 seeks to regulate the use of Aadhaar for targeted delivery of subsidies and services. It prohibits the use of Aadhaar information for purposes other than those specified in the Act. It establishes the UIDAI as the regulatory authority and criminalises unauthorised disclosure of identity information. However, critics have argued that the Act's safeguards are inadequate. The Act does not provide any right to individuals to access their own data held by the UIDAI, and its consent framework is weak. More fundamentally, the very act of collecting and centralising biometric data of over a billion people creates structural vulnerabilities that no statutory safeguard can fully address.

3.5 Aadhaar and the Private Sector

One of the most constitutionally significant developments in the Aadhaar story is the extension of the system to the private sector. Section 57 of the original Aadhaar Act permitted private entities to use Aadhaar authentication for purposes specified by them, subject to regulations framed by the UIDAI. This provision effectively allowed corporations to build

ISSN: 2582-6433

commercial surveillance systems on top of the state's biometric infrastructure. Financial institutions, telecom companies, and digital platforms used Aadhaar e-KYC (Know Your Customer) to authenticate users. This blurring of the line between state and private surveillance substantially amplified the privacy risks associated with Aadhaar.10

Chapter 4: Biometric Surveillance and Fundamental Rights

4.1 The Nature of Biometric Data

Biometric data is inherently different from other forms of personal data. Unlike a name, address, or identification number, biometric identifiers such as fingerprints and iris scans are permanently attached to the physical body of an individual. They cannot be changed in case of compromise. They are uniquely individual and cannot be anonymised in any meaningful sense. Once collected and stored in a centralised database, biometric data becomes a permanent feature of a person's identity that is wholly outside the person's control. This permanence and irreplaceability make the protection of biometric data a matter of profound constitutional significance.11

4.2 Biometric Surveillance and the Right to Bodily Integrity

Article 21's protection of personal liberty has been interpreted to include the right to bodily integrity. No person can be compelled to submit to a physical intrusion by the state without lawful justification. The compulsory collection of fingerprints and iris scans involves a physical act directed at the individual's body. Even though the physical discomfort is minimal, the constitutional dimensions are significant: the state is effectively appropriating a part of the individual's biological identity. Courts in several countries have recognised that compelling biometric enrolment engages bodily integrity rights, and that such compulsion requires compelling justification.

4.3 Informational Privacy and the Surveillance Architecture

The privacy implications of Aadhaar extend well beyond the moment of enrolment. The authentication architecture creates what scholars have called a 'surveillance infrastructure.' Every authentication generates a log at the central server. If an individual uses Aadhaar to access rations, pay taxes, receive a pension, or visit a hospital, a record of that interaction is preserved in the UIDAI's systems. Over time, these records aggregate into a detailed profile of an individual's economic activity, health conditions, location patterns, and lifestyle. This 'data profile' constitutes a form of state surveillance that fundamentally alters the citizen-state

ISSN: 2582-6433

relationship.12

4.4 The Chilling Effect on Rights

Surveillance has a well-documented chilling effect on the exercise of fundamental freedoms. When individuals know that their interactions with the state are being monitored and recorded, they may modify their behaviour to avoid attracting attention. A political activist who fears that her welfare benefit claims are being tracked may hesitate to associate with dissident movements. A marginalised community member may avoid accessing health services if she fears that her biometric data could be used against her in other contexts. The chilling effect of surveillance on freedoms of expression, association, and movement is not speculative; it is a constitutionally recognised harm.13

4.5 The Right Against Self-Incrimination

Article 20(3) of the Constitution provides that no person accused of any offence shall be compelled to be a witness against himself. In Selvi v. State of Karnataka (2010), the Supreme Court held that compelling a person to undergo scientific tests that extract testimonial information from the person violates Article 20(3).14 While the Aadhaar authentication is not specifically directed at criminal suspects, the systematic collection and storage of biometric data in a state database, and the potential use of that data in criminal investigations, raises serious concerns under Article 20(3). The architecture of Aadhaar creates a permanent record of biometric identity that could, in theory, be used as evidence against individuals in a range of proceedings.

4.6 The Right to Equality and Exclusion

Paradoxically, a system designed to promote inclusion has become a source of exclusion for India's most vulnerable citizens. Reports from across the country document cases of elderly individuals whose fingerprints have degraded with age and who cannot authenticate; persons with disabilities whose biometric features do not register on scanners; manual labourers whose biometrics do not match stored records due to work-related wear. When these individuals cannot authenticate, they are denied food rations, pensions, and other entitlements. This denial of subsistence amounts to a deprivation of the right to life under Article 21, caused not by deliberate state action but by the structural design of the authentication system.15

ISSN: 2582-6433

Chapter 5: Judicial Journey – The Puttaswamy Cases

5.1 Background to the Aadhaar Litigation

The constitutional challenge to Aadhaar came in multiple waves. The earliest challenges were filed even before the Aadhaar Act was enacted, by retired Justice K.S. Puttaswamy and others who contended that the collection of biometric data violated the right to privacy. The Supreme Court, by 2015, had referred the question of whether privacy was a fundamental right to a nine- judge bench, recognising that the answer was foundational to the Aadhaar challenge.

5.2 The Privacy Judgment (2017)

As discussed in Chapter 2, the nine-judge bench in K.S. Puttaswamy v. Union of India (2017) unanimously resolved the foundational question by holding that privacy is a fundamental right.6 The judgment was not a direct ruling on Aadhaar, but it established the constitutional framework within which Aadhaar would have to be assessed. By recognising informational privacy, bodily integrity, and the right to control one's own data as components of the fundamental right to privacy, the Court set a high bar that the Aadhaar architecture would need to clear.

5.3 The Aadhaar Judgment (2018)

A five-judge constitutional bench delivered its verdict on the Aadhaar Act in K.S. Puttaswamy v. Union of India (Aadhaar-5J Bench) in 2018.16 The majority upheld the constitutional validity of Aadhaar as a project and of the Aadhaar Act, 2016, subject to several conditions. The Court held that Aadhaar served a legitimate state purpose in targeting welfare delivery, and that the informational security measures in the Act — including the prohibition on sharing Aadhaar data and the requirement of consent for authentication — were sufficient to protect privacy in the welfare context.

However, the Court struck down several important provisions. Section 57, which allowed private entities to use Aadhaar for authentication, was struck down as unconstitutional because it permitted commercial surveillance of citizens by private parties without adequate safeguards. The mandatory linkage of Aadhaar with bank accounts and mobile phones — imposed by executive direction rather than legislative mandate — was also invalidated. The Court further struck down the use of Aadhaar authentication for services provided by private entities, holding that private surveillance is fundamentally different from state surveillance and requires independent constitutional justification.

ISSN: 2582-6433

5.4 Justice Chandrachud's Dissent

Justice D.Y. Chandrachud wrote a powerful dissent in the Aadhaar case, taking a far more critical view of the Aadhaar architecture.17 He held that the Aadhaar Act was unconstitutionally enacted as a Money Bill, since it contained provisions that were not related to taxation or expenditure. On the merits, he argued that the centralised biometric database created a permanent and irreversible surveillance infrastructure, that the authentication logs enabled the state to construct detailed profiles of citizens, and that no amount of statutory safeguards could adequately protect against the structural risks of such a system. He also expressed concern about the normative choice to treat citizens as subjects of biometric identification rather than as bearers of rights.

5.5 Post-Aadhaar Judicial Developments

Subsequent to the 2018 judgment, courts have continued to grapple with the implications of biometric identity systems. The Supreme Court has, in various decisions, emphasised the need for proportionality in data collection and has flagged the absence of a comprehensive data protection law as a significant gap in the constitutional framework. The Personal Data Protection Bill, discussed in several forms since 2018 before eventually passing as the Digital Personal Data Protection Act, 2023, represents the legislature's attempt to address some of these concerns, though with significant limitations.

Chapter 6: Continuing Constitutional Concerns Post-Puttaswamy

6.1 The Surveillance Infrastructure Persists

Despite the partial victories in the 2018 Aadhaar judgment, the structural concerns about biometric surveillance have not been resolved. The centralised biometric database maintained by the UIDAI continues to exist and continues to grow. Authentication logs continue to be generated. The government has not enacted comprehensive legislation governing the collection, use, retention, and deletion of biometric data. In the absence of such legislation, the constitutional protection of privacy remains incomplete and dependent on judicial intervention rather than legislative guarantee.

6.2 The Digital Personal Data Protection Act, 2023 and Its Limitations

The Digital Personal Data Protection Act, 2023 was enacted with the stated purpose of protecting personal data and providing a framework for its processing.18 While the Act is a significant step forward in some respects, it has drawn sharp criticism from data protection

ISSN: 2582-6433

scholars and civil liberties advocates. The Act does not treat biometric data as a special category of sensitive data requiring heightened protection. It grants the central government sweeping powers to exempt government entities from the Act's provisions, which effectively excludes the state from accountability under the very law designed to regulate data processing. This exemption is deeply problematic from a constitutional standpoint because it is precisely state-conducted surveillance that poses the greatest threat to the right to privacy.

6.3 The Problem of Mission Creep

One of the most persistent concerns in the Aadhaar debate is the risk of mission creep — the gradual expansion of a system's use beyond its originally stated purpose. Aadhaar was introduced as a mechanism for targeted welfare delivery. It has since been used for tax compliance, law enforcement, judicial processes, and private commercial authentication. Each expansion involves a new purpose for which the individual did not originally consent and which may involve different and more serious privacy implications. Mission creep is constitutionally significant because the proportionality analysis applicable to welfare delivery is not the same as that applicable to law enforcement or criminal investigation.19

6.4 The Absence of an Independent Data Regulator

A rights-protective biometric surveillance system requires an independent regulatory authority with genuine powers of oversight, investigation, and enforcement. The UIDAI, which was created to promote and manage the Aadhaar system, cannot credibly serve as a neutral regulator of that same system. The conflict of interest is structural. India currently lacks an independent data protection authority with real investigative and adjudicatory powers. The Data Protection Board proposed under the Digital Personal Data Protection Act, 2023, has not yet been fully operationalised, and its independence from the executive has been questioned.

6.5 Exclusion and Authentication Failures

Authentication failures in the Aadhaar system continue to result in denial of entitlements to vulnerable populations. Farmers, the elderly, persons with disabilities, and daily wage workers who are unable to authenticate biometrically are systematically excluded from welfare benefits. These exclusions have in some documented cases resulted in starvation deaths among persons who could not access food rations due to Aadhaar authentication failures. The constitutional implications are grave: the state's technological choices are resulting in the deprivation of the right to life under Article 21 for the most marginalised citizens. This is not a

ISSN: 2582-6433

peripheral technical failure but a fundamental structural flaw in the design of the system.20

6.6 Surveillance Expansion Beyond Aadhaar

The Aadhaar system does not exist in isolation. It is increasingly integrated with other surveillance technologies including facial recognition systems being deployed by police departments across India, CCTV networks in public spaces, and proposed vehicle tracking systems. The integration of biometric identity data with these surveillance technologies creates a comprehensive surveillance architecture that goes far beyond anything that the Aadhaar Act contemplated or that the Supreme Court addressed in 2018. The constitutional implications of this integrated surveillance state demand urgent legislative and judicial attention.

Chapter 7: Comparative Perspectives

7.1 The European Union: GDPR and Biometric Data Protection

The European Union's General Data Protection Regulation (GDPR), adopted in 2016 and effective from 2018, provides the most comprehensive framework for the protection of personal data in the world.21 Under the GDPR, biometric data processed for the purpose of uniquely identifying a natural person is treated as a special category of sensitive data, subject to heightened restrictions. The processing of such data is generally prohibited except where one of a limited number of specific conditions is met, including explicit consent or substantial public interest. The GDPR requires data minimisation, purpose limitation, storage limitation, and security measures proportionate to the sensitivity of the data. It also creates robust individual rights including the right of access, the right to rectification, and the right to erasure.

India's legal framework falls significantly short of the GDPR standard. The Digital Personal Data Protection Act, 2023 does not treat biometric data as a special category and does not impose the same level of restrictions on state-conducted data processing. The contrast with the European approach is instructive: the EU treats the protection of personal data as a fundamental right deserving the highest level of protection, while India's current framework treats it primarily as a regulatory compliance issue.

7.2 The United Kingdom: Regulation of Investigatory Powers

The United Kingdom has developed a legal framework for regulating the use of surveillance powers by state authorities through the Regulation of Investigatory Powers Act (RIPA) 2000 and its successor, the Investigatory Powers Act 2016.22 These statutes require judicial or quasi-judicial authorisation before surveillance powers can be exercised, establish

ISSN: 2582-6433

oversight bodies to review the use of surveillance, and provide remedies to individuals whose rights have been violated. The UK framework demonstrates that it is possible to give law enforcement agencies access to digital surveillance tools while maintaining meaningful accountability and judicial oversight.

7.3 The United States: Fourth Amendment and Biometric Surveillance

In the United States, the Fourth Amendment's protection against unreasonable searches and seizures has been applied by courts to regulate digital surveillance.23 The Supreme Court in Carpenter v. United States (2018) held that accessing historical cell-site location information requires a warrant, significantly extending Fourth Amendment protection to digital data. Several US states have enacted specific biometric privacy laws: the Illinois Biometric Information Privacy Act (BIPA) requires informed consent before collecting biometric data and creates a private right of action for violations. The BIPA has been used successfully to challenge the collection of biometric data by companies, resulting in significant settlements. India has no comparable statutory framework for biometric privacy.

7.4 Lessons for India

The comparative survey reveals a consistent pattern in democratic societies: biometric and digital surveillance by the state is treated as an inherently risky enterprise that requires specific legislative authorisation, judicial oversight, independent regulation, strong individual rights, and strict purpose limitation. India's current approach — a centralised biometric database, weak oversight, minimal individual rights, and a data protection law that largely exempts the state falls well short of the standards that India's own Constitution demands and that comparable democracies have implemented. Adopting elements of these international frameworks is not merely a matter of global alignment but of constitutional necessity.

Chapter 8: Towards a Rights-Based Framework – Recommendations

8.1 Introduction

The constitutional analysis in the preceding chapters establishes that India's current framework for Aadhaar-based biometric surveillance is constitutionally inadequate. It does not fully satisfy the proportionality standard established by the Privacy Judgment, does not provide meaningful individual rights over biometric data, lacks independent oversight, and structurally enables mission creep. This chapter proposes a set of concrete legal and institutional reforms that are necessary to bring the biometric governance framework into harmony with Article 21

ISSN: 2582-6433

and the broader constitutional framework of fundamental rights.

8.2 Enact a Comprehensive Biometric Data Protection Law

India requires a dedicated statute governing the collection, use, storage, and deletion of biometric data, separate from and in addition to the general Digital Personal Data Protection Act. This statute should categorise biometric data as uniquely sensitive and deserving of the highest level of protection. It should require explicit, informed, and revocable consent for the collection of biometric data; prohibit the use of biometric data for purposes other than those for which consent was given; establish maximum retention periods; require the deletion of biometric data when the identified purpose ceases to exist; and create a private right of action for individuals whose biometric privacy has been violated.

8.3 Establish an Independent Biometric Data Protection Authority

The UIDAI cannot simultaneously promote Aadhaar and regulate its use. India needs an independent Biometric Data Protection Authority, insulated from executive control, with powers to investigate complaints, conduct audits of UIDAI and other biometric data processors, impose penalties for violations, and recommend legislative reforms. The independence of this authority from the government of the day is a constitutional requirement, not merely a matter of administrative design. Without independent oversight, the right to privacy cannot be effectively enforced against state surveillance.

8.4 Judicial Authorisation for Surveillance Uses of Biometric Data

Any use of Aadhaar biometric data for law enforcement, intelligence, or surveillance purposes should require prior judicial authorisation. The decision to access an individual's biometric records for purposes beyond the original welfare-delivery mandate involves a significant privacy intrusion that must be subject to independent scrutiny. A framework similar to the warrant requirement in criminal procedure should be established, requiring police and intelligence agencies to demonstrate probable cause before accessing biometric authentication logs or other Aadhaar records.

8.5 Mandatory Alternatives to Biometric Authentication

The constitutional vulnerability arising from biometric authentication failures can be addressed by requiring that all services and entitlements for which Aadhaar authentication is used must also offer robust alternatives that do not depend on biometric matching. These

ISSN: 2582-6433

alternatives should be genuinely accessible, not treated as inferior or stigmatised options. The availability of meaningful alternatives is essential to ensure that the design of the authentication system does not, in effect, deprive the most vulnerable citizens of their constitutional right to life and livelihood.

8.6 Sunset Clauses and Periodic Review

Given the rapidly evolving nature of biometric and surveillance technology, any statutory framework must build in mechanisms for periodic review. Parliament should mandate that the use of biometric data collection programmes be reviewed every five years against current technological realities, human rights standards, and constitutional requirements. Sunset clauses should be introduced for particularly invasive provisions, requiring positive legislative renewal rather than passive continuation.

8.7 Decentralisation of the Biometric Database

The centralised design of the UIDAI biometric database creates a single point of catastrophic failure: a successful attack on the database would expose the immutable biometric data of over a billion people. Constitutional proportionality requires that the state adopt the least invasive means capable of achieving its legitimate aim. Decentralised or federated biometric storage architectures, or the use of biometric data to generate irreversible cryptographic tokens rather than storing the raw biometrics, would significantly reduce the risk while preserving the utility of the system. The state's failure to explore and adopt these less invasive alternatives is itself a constitutional concern.

8.8 Public Legal Awareness

A rights-based biometric governance framework must also invest in public legal literacy. Citizens must be made aware of their rights over their own biometric data, the procedures through which they can challenge unauthorised use, and the remedies available to them. Legal aid organisations, civil society groups, and universities have a role to play in this education. A state that collects the biometric data of all its residents while keeping those residents ignorant of their rights over that data cannot credibly claim to be operating within a constitutional framework of consent and autonomy.

ISSN: 2582-6433

Chapter 9: Empirical Survey Analysis

9.1 Introduction

To supplement the doctrinal analysis in this paper, a small-scale survey was conducted among students and academic professionals in the Lucknow region. The survey was designed to assess ground-level awareness of the Aadhaar system, the right to privacy, and the constitutional concerns associated with biometric surveillance. A total of 45 respondents participated. The survey was administered through a structured questionnaire comprising twelve questions.

9.2 Respondent Profile

Of the 45 respondents, 38 (84.4%) were in the 18–25 age group, 5 (11.1%) were between

26 and 35, and 2 (4.4%) were above 35. By occupation, 36 respondents (80%) were law or humanities students, 6 (13.3%) were researchers or faculty members, and 3 (6.6%) were working professionals. The survey therefore reflects primarily the perspectives of the student population, though with some academic input.

9.3 Question-wise Analysis

Question 1: Are you enrolled in Aadhaar? Yes: 45 respondents (100%). This confirms universal enrolment among respondents, reflecting the de facto mandatory nature of Aadhaar for Indian residents.

Question 2: Were you explained your rights before enrolling in Aadhaar? Yes: 6 respondents (13.3%). No: 31 respondents (68.9%). Somewhat: 8 respondents (17.8%). This finding suggests that the consent process at enrolment is deeply deficient, with fewer than one in seven respondents having received meaningful information about their rights.

Question 3: Are you aware that the right to privacy is a fundamental right under Article 21? Fully aware: 24 respondents (53.3%). Somewhat aware: 14 respondents (31.1%). Not aware: 7 respondents (15.6%). While a majority have some awareness of privacy as a fundamental right, nearly half lack a full understanding, indicating a significant legal literacy gap.

Question 4: Do you know that the Supreme Court has ruled on Aadhaar's constitutionality? Yes: 28 respondents (62.2%). No: 11 respondents (24.4%). Not sure: 6 respondents (13.3%). The Aadhaar judgment is relatively well known among the educated

ISSN: 2582-6433

population, though a significant minority remains unaware.

Question 5: Are you concerned about the government storing your biometric data? Very concerned: 26 respondents (57.8%). Somewhat concerned: 13 respondents (28.9%). Not concerned: 6 respondents (13.3%). A substantial majority express serious concern about biometric data storage, suggesting that the privacy implications of Aadhaar resonate with the general population.

Question 6: Have you experienced or heard of Aadhaar authentication failures? Personally experienced: 14 respondents (31.1%). Heard of others experiencing it: 22 respondents (48.9%). No: 9 respondents (20%). Authentication failure is a widely shared experience, with over 80% of respondents either personally affected or aware of others who have been.

Question 7: Should biometric data be treated as more sensitive than other personal data? Yes: 39 respondents (86.7%). No: 3 respondents (6.7%). Not sure: 3 respondents (6.7%). There is near-unanimous recognition among respondents that biometric data deserves heightened protection.

Question 8: Do you believe the UIDAI adequately protects your biometric data? Yes: 9 respondents (20%). No: 25 respondents (55.6%). Not sure: 11 respondents (24.4%). A majority doubt the adequacy of current data protection measures, reflecting widespread scepticism about institutional safeguards.

Question 9: Should an independent regulator oversee Aadhaar? Yes: 38 respondents (84.4%). No: 2 respondents (4.4%). Not sure: 5 respondents (11.1%). There is strong support for independent oversight, validating the recommendation in Chapter 8.

Question 10: Do you support mandatory alternatives to biometric authentication? Yes: 40 respondents (88.9%). No: 2 respondents (4.4%). Not sure: 3 respondents (6.7%). Overwhelming support for alternatives reflects awareness of the exclusion problem.

Question 11: Do you believe Aadhaar-based surveillance can be misused by the state? Yes: 36 respondents (80%). No: 5 respondents (11.1%). Not sure: 4 respondents (8.9%). Four out of five respondents fear state misuse, suggesting that public trust in the government's use of biometric data is limited.

Question 12: Should India enact a dedicated Biometric Data Protection Law? Yes: 41 respondents (91.1%). No: 1 respondent (2.2%). Not sure: 3 respondents (6.7%). Near-unanimous support for dedicated legislation is the most significant finding of the survey.

ISSN: 2582-6433

9.4 Key Findings Summary

- 100% of respondents are enrolled in Aadhaar, confirming de facto mandatory status.
- Only 13.3% were adequately informed of their rights at enrolment — consent is largely notional.
- 57.8% are very concerned about government storage of biometric data.
- 80% fear potential state misuse of biometric surveillance.
- 86.7% believe biometric data deserves heightened protection compared to other personal data.
- 84.4% support independent regulatory oversight of Aadhaar.
- 91.1% support a dedicated Biometric Data Protection Law.

9.5 Survey Conclusions

The survey findings strongly corroborate the doctrinal analysis in this paper. Public concern about biometric surveillance is widespread, trust in current institutional safeguards is low, and there is overwhelming popular support for stronger legal protections. The gap between the constitutional promise of privacy and the lived reality of Aadhaar enrolment — as reflected in the near-universal absence of informed consent — is perhaps the most troubling finding. It suggests that the constitutional framework, even after Puttaswamy, has not translated into meaningful protection at the level of everyday experience.

Chapter 10: Conclusion

10.1 Synthesis of the Research

This paper has examined the constitutional dimensions of Aadhaar-based biometric surveillance in India through the lens of the right to privacy under Article 21. It has traced the evolution of Article 21 from a narrow procedural guarantee to a rich substantive right encompassing dignity, bodily integrity, informational autonomy, and the freedom to be left alone. It has analysed the architecture of the Aadhaar system, the constitutional challenges it presents, the Supreme Court's treatment of those challenges, and the continuing gaps in India's legal framework for biometric governance.

10.2 The Central Finding

The central finding of this paper is that while the Supreme Court's 2018 judgment in the Aadhaar case addressed some of the most egregious constitutional infirmities of the original system, the fundamental structural concerns remain unresolved. A centralised biometric

ISSN: 2582-6433

database of over a billion people, governed by a law that does not treat biometric data as specially sensitive, overseen by an authority that is neither independent nor adequately accountable, and expanding through integration with other surveillance technologies, does not satisfy the constitutional requirements of the proportionality test established by the Privacy Judgment.

10.3 The Gap Between Law and Reality

The empirical survey confirms what the doctrinal analysis suggests: the constitutional promise of the right to privacy has not translated into meaningful protection for ordinary citizens in their encounters with the Aadhaar system. Consent is notional, exclusion from entitlements due to authentication failures is widespread, and public trust in institutional safeguards is low. The law on paper and the law in practice are separated by a significant gap that legislative and institutional reform must bridge.

10.4 Constitutional Values as a Guide

Technology is not neutral. The choice to build a centralised biometric database, to mandate its use as a condition for accessing rights, and to allow its expansion into an integrated surveillance infrastructure reflects a particular vision of the relationship between the state and the citizen. This paper has argued that this vision is in tension with the constitutional vision of the individual as a bearer of fundamental rights who cannot be reduced to a data point in a government database. Article 21, as interpreted by the Supreme Court, demands that the individual's dignity, autonomy, and privacy be treated not as inconveniences to be managed but as the constitutional core that must constrain and guide the state's technological choices.

10.5 Final Observations

The legitimacy of the Aadhaar system, and of the biometric surveillance architecture that has grown around it, ultimately depends on whether it is governed by a legal framework that takes privacy seriously as a fundamental right. That framework does not yet exist in India. Building it requires legislative commitment, institutional design, judicial vigilance, and civic engagement. The recommendations in this paper offer a starting point. The constitutional imperative, however, is clear: a state that holds the biometric identity of every one of its residents must govern that power with the highest standards of legal accountability, transparency, and respect for the rights it is bound by oath to protect.

A state that uses technology to govern must still be a state governed by the Constitution.

ISSN: 2582-6433

Privacy is not a privilege that the state grants; it is a fundamental right that the state must respect. Aadhaar, in its present form, has not fully crossed that threshold. India's constitutional future requires that it does.

Footnotes

a) India Const. art. 21.
b) A.K. Gopalan v. State of Madras, AIR 1950 SC 27.
c) Maneka Gandhi v. Union of India, (1978) 1 SCC 248.
d) Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.
e) Gobind v. State of Madhya Pradesh, (1975) 2 SCC 148.
f) K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (Privacy Judgment).
g) Id. at ¶¶ 180–185 (Chandrachud, J., concurring) (articulating the four-part proportionality test).
h) Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, No. 18, Acts of Parliament, 2016 (India).
i) See Reetika Khera (ed.), The Battle for Employment Guarantee (2011) (documenting exclusion from welfare due to mandatory Aadhaar linkage).
j) Aadhaar Act, 2016, § 57 (struck down by the Supreme Court in 2018).
k) See Paul M. Schwartz & Daniel J. Solove, The PII Problem: Privacy and a New Concept of Personally Identifiable Information, 86 N.Y.U. L. Rev. 1814 (2011).
l) Shyam Divan & Usha Ramanathan, Identification, Surveillance and Welfare: The Aadhaar Debate in India (2019).
m) People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301 (discussing surveillance and civil liberties).
n) Selvi v. State of Karnataka, (2010) 7 SCC 263.
o) Jean Drèze & Nazar Khalid, Aadhaar and Food Security in Jharkhand: Pain Without Gain, 52 Economic & Political Weekly 50 (2017).
p) K.S. Puttaswamy v. Union of India, (2019) 1 SCC 1 (Aadhaar five-judge bench judgment).
q) Id. (Chandrachud, J., dissenting).
r) Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
s) See Lawrence Lessig, Code: Version 2.0 (2006) (discussing technological design and legal regulation).
t) See Nikhil Dey et al., Aadhaar and the Right to Food: Exclusions in Rajasthan, Centre

ISSN: 2582-6433

for Equity Studies Report (2018).

u) Council Regulation (EU) 2016/679 of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data (General Data Protection Regulation), 2016 O.J. (L 119) 1.

v) Investigatory Powers Act 2016, c. 25 (UK).

w) Carpenter v. United States, 585 U.S. 296 (2018).

Bibliography

Constitutional and Statutory Provisions

India Const. art. 21 (Right to Life and Personal Liberty). India Const. art. 20(3) (Protection against Self-Incrimination).

Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, No. 18, Acts of Parliament, 2016.

Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023. Information Technology Act, 2000, No. 21, Acts of Parliament, 2000.

Judicial Decisions

A.K. Gopalan v. State of Madras, AIR 1950 SC 27.

Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295. Gobind v. State of Madhya Pradesh, (1975) 2 SCC 148.

Maneka Gandhi v. Union of India, (1978) 1 SCC 248.

People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301. Selvi v. State of Karnataka, (2010) 7 SCC 263.

K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (Privacy Judgment).

K.S. Puttaswamy v. Union of India, (2019) 1 SCC 1 (Aadhaar Judgment). Carpenter v. United States, 585 U.S. 296 (2018) (USA).

Books

Reetika Khera (ed.), The Battle for Employment Guarantee (OUP 2011).

Shyam Divan & Usha Ramanathan, Identification, Surveillance and Welfare: The Aadhaar Debate in India (2019).

Lawrence Lessig, Code: Version 2.0 (Basic Books 2006).

Paul M. Schwartz & Daniel J. Solove, Information Privacy Law (5th ed., Wolters Kluwer 2015).

ISSN: 2582-6433

S.N. Jain, Theoretical and Non-Theoretical Legal Research (Deep & Deep Publications 2009).

Journal Articles and Reports

Jean Drèze & Nazar Khalid, Aadhaar and Food Security in Jharkhand: Pain Without Gain, 52 Economic & Political Weekly 50 (2017).

Nikhil Dey et al., Aadhaar and the Right to Food: Exclusions in Rajasthan, Centre for Equity Studies Report (2018).

Paul M. Schwartz & Daniel J. Solove, The PII Problem: Privacy and a New Concept of Personally Identifiable Information, 86 N.Y.U. L. Rev. 1814 (2011).

Usha Ramanathan, A Unique Identity Bill, 45 Economic & Political Weekly 10 (2010).

Vrinda Bhandari & Amber Sinha, The Aadhaar Judgment and the Future of Privacy in India, 10 Indian Journal of Law & Technology 1 (2019).

International Instruments

Council Regulation (EU) 2016/679 (General Data Protection Regulation), 2016 O.J. (L 119) 1.

Investigatory Powers Act 2016, c. 25 (UK).

Illinois Biometric Information Privacy Act, 740 ILCS 14 (2008) (USA).

UN General Assembly, The Right to Privacy in the Digital Age, UN Doc A/RES/68/167 (December 2013).