INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW
An International Open Access Double Blind Peer Reviewed, Referred Journal

Volume 5 | Issue 1 | 2026 Art. 15

An Analysis of Puttaswamy: The Supreme Court Privacy Verdict with Reference to Aadhar Card

Saras Yadav
Law Student
Amity Law School, Amity University, Lucknow

Dr. Srijan Mishra
Assistant Professor
Amity Law School, Amity University, Lucknow

Recommended Citation
Saras Yadav and Dr. Srijan Mishra, *An Analysis of Puttaswamy: The Supreme Court Privacy Verdict with Reference to Aadhar Card*, 5 IJHRLR 219-238 (2026).
Available at www.humanrightlawreview.in/archives/.

An Analysis of Puttaswamy: The Supreme Court Privacy Verdict with Reference to Aadhar Card

Saras Yadav
Law Student
Amity Law School, Amity University, Lucknow

Dr. Srijan Mishra
Assistant Professor
Amity Law School, Amity University, Lucknow

Manuscript Received	Manuscript Accepted	Manuscript Published
21 Jan. 2026	24 Jan. 2026	04 Feb. 2026

ABSTRACT

This paper discusses the Supreme Court's framing of the fundamental right to privacy in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) and what that means for the Aadhaar program in the 2018 Aadhaar verdict (Puttaswamy II). The nine-judge court, by its judgment in 2017, held that privacy is vital to life and personal liberty under Article 21 and inherent in the remainder of Part III, thereby overruling earlier decisions in M.P. Sharma and Kharak Singh that had limited the applicability of constitutional privacy. The Constitution Bench, in 2018, applied a structured proportionality review—focusing on legality, legitimate purpose, necessity, and balancing—to examine how various aspects of Aadhaar conform to or clash with privacy and dignity. Doctrinal analysis is interspersed with a normative assessment of Aadhaar's implementation, flagging data collection, storage, authentication, and linkage requirements, especially linked to welfare benefits, PAN, bank accounts, and mobile connections. The paper concludes that the Court viewed Aadhaar as a valid welfare tool and approved its use for subsidies and PAN linkage but restricted its use in the private sector, struck down provisions enabling widespread data sharing and prolonged retention, and held mandatory linkage with bank accounts and mobile numbers to be disproportionate. The analysis finds that Puttaswamy has been a game-changer for Indian constitutional law in terms of bringing about an enhanced informational privacy and data protection, but at the same time, it has raised very serious questions on exclusion, profiling, and the adequacy of the existing

statutory regime, which essentially brings into sharp focus the need for robust data protection legislation and continued judicial oversight.

KEYWORDS

Right to Privacy, Aadhaar Scheme, Puttaswamy Judgment, Proportionality Test, Informational Privacy, Data Protection

INTRODUCTION

Aadhaar, formed in 2009 with the Unique Identification Authority of India (UIDAI) leadership, had originally been conceptualized to provide a technology solution to the societal issue of duplication, leaks, and inefficient use seen in the Indian social welfare distribution system. This initiative attempted to simplify the distribution process using a unique identification number based on biometric information to achieve social inclusion objectives to provide subsidized services effectively to each citizen. However, originally conceptualized to be an idea derived from technology to solve a State-imposed problem, Aadhaar has developed into a constitutional issue with the use of biometric information affecting serious constitutional issues with State control in the surveillance State.[1]

Aadhaar has been accused of reshaping the State-citizenry dynamic to transform people into data points to enable unbridled surveillance of citizens' private lives by the State government. On the other hand, Aadhaar has been described to be "an inclusive architecture—a device of empowerment to those who hitherto lacked access to State services protected by the Constitution."[2]

This schism brought Aadhaar to the crucial intersection of two visions of the constitution: one which privileged efficiency and inclusivity through technology, and another which held dignity and privacy as essences of personality. The constitutional challenge to Aadhaar arose from a peculiar jurisprudential vacuum. The Indian Supreme Court is yet to recognise privacy as an essential right. The earlier Supreme Court judgments have been 'equivocal' and 'sometimes contradict'.

In M.P. Sharma v. Satish Chandra (1954), an eight-judge bench held that 'the constitution does not enlarge the right to privacy' and that 'the provisions relating to search and seizure contained

[1] Columbia Global Freedom of Expression. (2023). *Puttaswamy v. Union of India (II).*
[2] Oxford Human Rights Hub. (2017). *Defining the Right to Privacy in India in light of Justice K.S. Puttaswamy*

in Articles 20(3) and 22(3) of the Indian Constitution do not support' any universal claim for privacy. In similar fashion to M.P. Sharma v. Satish Chandra, the Court rejected police surveillance on 'the limited concept of "Personal Liberty" flowing from Articles 14 and 21' in *Kharak Singh v. State of Uttar Pradesh (1963),* obviously rejecting 'the notion of "a peculiar and special right of privacy" peculiar to themselves.'

By the mid-2010s, growing coverage of the UIDAI and the enactment of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act, 2016, brought privacy concerns to the fore. The petitioners were of the view that the storage of such information by the State without constitutionally cognizable privacy protections amounted to mass surveillance. The issue was framed by a bench of three judges in 2015, who agreed to revisit earlier judgments and referred the issue of recognizability of privacy being a basic right under the Constitution to a full bench and led to the historic nine-member bench decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India in 2017.*

In the *2017 Puttaswamy Decision*, the right to privacy is "inextricably linked" to life and liberty under Article 21 of the Indian Constitution and is also derived from other elements of part III and grounds of freedom encompassed in Article 19 and equality under Article 14. Privacy is visualized as "the essence of human dignity," and there are three interlocking spheres of privacy: bodily privacy covering bodily integrity and spatiality, decisional privacy treating freedom of choice in personal and familial affairs, and finally, formational privacy dealing with personal data processing and its usage. This judgment effectively overturned M.P. Sharma and Kharak Singh and brought India in line with global jurisprudence concerning liberty and autonomy in realizing privacy as an essential component of liberty and autonomy and freedom of choice and dignity of human life.[3]

More importantly, Puttaswamy suggested an organized form of proportionality analysis to assess the limits of privacy. & quot ; Any intrusion into the right to privacy must satisfy four elements:

(1) Legality— Existence of constitutional or legal provision;
(2) Legitimate aim—Compelling state object;
(3) Necessity—Least intrusive techniques; and
(4) Balancing—Proportionality between right violation and state object.

[3] Supreme Court Observer. (2023). *Constitutionality of Aadhaar Act: Judgment Summary*.

This approach equips the court with an analysis system to treat privacy concerns not just as an absolute prohibition but rather as context-specific assessments of necessity and proportionality. This kind of analysis system would later become the guiding principle for testing the constitutional validity of Aadhaar in 2018.

When this five-judge bench re-evaluated Aadhaar in ***Puttaswamy (Aadhaar II, 2018),*** it was faced with different constitutional strands. One strand represented Aadhaar as an agent of empowerment—a device to rationalize welfare spending, eliminate corruptions, and fulfil socio-economic rights through Articles 38, 39, and 41 of the Indian Constitution. At the opposite end was the fear of a "database State," wherein biometric and demographic data could be abused for purposes of surveillance and targeting. The court was thus forced to balance efficiency and empowerment against privacy and liberty under this newly crafted test of proportionality.[4]

The majority decision, led by Chief Justice Dipak Misra and Justice Sikri, validated the constitutional provision of the Aadhaar Act, holding that it was for a valid governmental purpose: ensuring targeted allocation of social allowances from the Consolidated Fund of India. The Court recognized the government's submission that Aadhaar's architecture, with adequate legislative and regulatory mechanisms in place, adequately addressed risks in the exploitation of data. Nevertheless, this decision also set important boundaries. It struck down Section 57, which allowed private entities to make use of Aadhaar authentication, declared Aadhaar-WeChat, Aadhaar-mobile, Aadhaar-banking, and Aadhaar-PAN number links unconstitutional, and shortened data preservation terms from five to six months. These measures were necessary, it declared, to maintain the KYC function of Aadhaar. On the other hand, Aadhaar-PAN linkage was held necessary for preventing evasion and deterring individuals from holding more than one identity.

Jagadesh's dissenting opinion saw Justice D. Y. Chandrachud hold that "the entire Aadhaar edifice…is illegal." He argued that "the legislative ambition expressed through Section 123(2) of the Act has sidestepped the principles of democracy" through being a Money Bill. Moreover, it "constitutes an existential threat to the principles of informational self-determination." The opposition articulated Aadhaar not just in privacy terms but also on constitutional matters of governance, wherein an imbalance of power between State and individual was institutionalized through

[4] Supreme Court Observer. (2025). *Fundamental Right to Privacy – Case Background (Puttaswamy*

its structure. This study completes the gap existing in previous research on these two significant judgments: ***Puttaswamy I,*** regarding the right to privacy, and ***Puttaswamy II,*** regarding privacy in fact. Both these areas have generally been investigated independently by scholars, either from the paradigm of constitutional ideas or else by case analyses related to public policies. In truth, it was these two aspects of dialogue about abstract ideas of dignity, autonomy, and proportions which were applicable, given that the Court was applying these notions to India's most extensive welfare surveillance system. As shown by the 2025 study by IJFMR, the Aadhaar judgment was clearly the test case for whether the right to privacy was able to circumscribe the surveillance-welfare nexus. Three key objectives drive this research. Firstly, to clarify how the Supreme Court understands the concept of right to privacy in Puttaswamy and its implications for digital governance in general. Secondly, to analyse how this understanding made a difference in the Court's reasoning while determining Aadhaar's validity, particularly in light of proportionality. Thirdly, to examine if a holistic balancing mechanism allowed for a sustainable scope of informational privacy with a legitimate welfare objective on the Court's part. "The central argument that is advanced in this work is that, while Puttaswamy I established a robust, dignity-focused privacy paradigm and the proportionality principle as a mechanism for adjudicating rights, the judicial stance on Aadhaar II has shown a degree of judicial ambivalence.

According to this, the judicial posture towards the state's claims of benefit and efficient delivery has engendered a partial constitutionalizing of informational privacy, where particular instances of abuse might be discounted but the rationale of Aadhaar was maintained. In this way, informational privacy is guaranteed in theory but vulnerable in practice, beset by a lack of transparency, inadequate monitoring, and potential function creep." Finally, the Aadhaar judicial precedent illustrates the evolutionary character of privacy itself and the development of the Indian Constitution. It reflects that the predominant progress is even from the negative to the affirmative recognition but not to the institutionalization. Moreover, with the growing presence of biographic identification and analysis and algorithmic governance, the scope of the Puttaswamy case is more relevant with respect to the future ideals rather than the present rulings and visions. Consequently, the Aadhaar experience can be most aptly termed as the developing experience and not the decided experience. This depends on the success and realization that the growing new generations may correlate the Puttaswamy vision

and ideals with the reality of the digital India.[5]

METHODS

This study utilizes a predominantly doctrinal research approach, supported with normative and policy analysis of Aadhaar's functioning within India's welfare and digital governance infrastructure. The doctrinal component involves close reading of the full text of Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) and Justice K.S. Puttaswamy (Aadhaar) v. Union of India (2018), including the majority, concurring, and dissenting opinions, with a focus on how each opinion theorises privacy, proportionality, and the role of the State in data driven governance. Key precedents on privacy and surveillance—such as M.P. Sharma, Kharak Singh, and subsequent decisions based on Puttaswamy—are studied to locate the verdicts within the wider trajectory of Indian constitutional law.[6]

Secondary resources include scholarly publications, case notes, and opinions from legal blogs and human rights groups, which give critical viewpoints on the implications of the privacy ruling and the Aadhaar decision. Reports and summaries from platforms such as Supreme Court Observer, Human Rights Watch, and Columbia Global Freedom of Expression are employed to capture the practical ramifications of the rulings and major doctrinal changes. Policy focused assessments describing the operation of Aadhaar, including its role in welfare delivery, PAN linking, and KYC procedures, are also addressed to contextualise the legal results.[7]

The participants in this analysis are institutional rather than individual: the Supreme Court as an interpreter of constitutional norms; the Unique Identification Authority of India (UIDAI) and government ministries as implementers of Aadhaar; and affected populations as represented through petitions, affidavits, and civil society critiques. No empirical survey or quantitative dataset is employed; instead, the research focuses on qualitative evaluation of official judgments, legislative language (Aadhaar Act, 2016; rules), and recorded implementation difficulties such as mandated links, authentication failures, and data breaches. Reproducibility is achieved by anchoring each stage of the analysis on citable original sources (judgments, laws) and readily

[5] Supreme Court Observer. (2025). *Aadhaar Review – Case*
[6] https://www.scconline.com/blog/post/2017/08/24/9-judge-bench-declares-privacy-as-a-fundamental-right-information-family-life-sexual-orientation-are-all-part-of-privacy-judgment/
[7] https://lawfullegal.in/the-landmark-aadhaar-judgment-2018-a-delicate-balance-between-empowerment-and-privacy/

available secondary commentary.[8]

RESULTS

Doctrinal Consequences of Puttaswamy (2017) - The nine judge bench in Puttaswamy (2017) reached a unanimous verdict with many concurring views, stating that the right to privacy is a basic right guaranteed under Part III of the Constitution, notably under Article 21's protection of life and personal liberty. The Court specifically invalidated prior dicta in M.P. Sharma and Kharak Singh to the extent that those cases denied or diminished a universal right to privacy, effectively addressing a long standing doctrinal question.[9]

The judgment conceptualised privacy in three overlapping dimensions: (a) bodily and physical privacy, including control over one's body and spaces; (b) informational privacy, concerning the collection, processing, and dissemination of personal data; and (c) decisional autonomy, covering intimate choices about family life, sexuality, and identity. Privacy was related closely to dignity and autonomy, with the Court identifying, among example, sexual orientation as an important element of privacy, predicting the eventual decriminalisation of consenting same sex relations in Navtej Johar.[10]

Importantly, the Court endorsed a structured proportionality test for evaluating restrictions on privacy, requiring: (1) existence of a valid law (legality); (2) a legitimate State aim; (3) rational connection and necessity, meaning that the measure is the least restrictive means; and (4) balancing between the extent of rights infringement and the importance of the goal. This standard was meant to guide future adjudication on data collecting, monitoring, and social systems, like Aadhaar.

Key holdings in Aadhaar (Puttaswamy II, 2018) - In the 2018 Aadhaar verdict, a 4:1 majority confirmed the constitutional legality of the Aadhaar Act, 2016, seeing Aadhaar as a lawful vehicle for targeted delivery of subsidies, benefits, and services paid by the Consolidated Fund of India. The Court ruled that Aadhaar pursues a legitimate State interest in avoiding leakages, removing duplicate and ghost beneficiaries, and promoting social and economic justice, therefore meeting the first components of

[8] Taxolawgy. (n.d.). *What was the 2018 Supreme Court Ruling on Aadhar Card?* Justice for All
[9] Supreme Court Observer. (2023). *Constitutionality of Aadhaar Act: Judgment Summary*.
[10] https://www.humandignitytrust.org/resources/puttaswamy-v-union-of-india-writ-petition-civil-no-494-of-2012/

the proportionality test.[11]

At the same time, the Court dismissed or read down certain clauses as unreasonable invasions into privacy:

- Section 57 was thrown down to the extent that it let private companies to utilize Aadhaar for verification, thereby preventing regular Aadhaar based KYC by private enterprises without a new, narrowly defined statute.
- Provisions and laws that authorized the keeping of authentication data for five years and the development of substantial metadata were deemed unlawful; retention beyond six months was pronounced prohibited to decrease profiling concerns.
- Mandatory linking of Aadhaar with bank accounts under the PMLA rules and with mobile numbers under Department of Telecommunications circulars was invalidated as failing the necessity and proportionality requirements, given the intrusive nature of financial and communication data and the availability of less restrictive alternatives.[12]

However, the Court affirmed obligatory linkage of Aadhaar with PAN under the Income Tax Act, stating that this step was reasonable to the legitimate objective of combating tax evasion and developing a solid taxpayer identification system. The majority also accepted the government's assertion that Aadhaar does not constitute a surveillance State since key biometric data are maintained in a centralized, purportedly secure system and are not immediately subject to profiling, a finding challenged by the opposition and many analysts.[13]
The dissenting opinion by Justice D.Y. Chandrachud took the opposite view on key points, characterising the Aadhaar Act as unconstitutional in its entirety, questioning its passage as a Money Bill, and arguing that the architecture of biometric identification and centralised databases is inherently incompatible with the right to anonymity and informational self-determination. For the dissent, the Aadhaar architecture failed the proportionality test since it facilitated ubiquitous, irreversible data collection and authentication based exclusion while delivering insufficient data security and monitoring[14]

[11] https://blog.finology.in/constitutional-developments/aadhaar-card-verdict
[12] Columbia Global Freedom of Expression. (2023). *Puttaswamy v. Union of India (II).*
[13] https://www.drishtiias.com/daily-news-analysis/supreme-court-upholds-aadhaars-constitutional-validity
[14] Taxolawgy. (n.d.). *What was the 2018 Supreme Court Ruling on Aadhar Card?* Justice for All.

Brief Written Expansion- The majority judgment constructs Aadhaar as a constitutionally acceptable welfare infrastructure, subject to tailored pruning of its most intrusive features. By upholding Aadhaar for subsidies and PAN linkage yet striking down bank/mobile linkages, Section 57, and expansive data-retention provisions, the Court projects itself as mediating between social-security objectives and privacy guarantees through the proportionality test.[15][16][17][18]

In contrast, Justice Chandrachud's dissent reads the same architecture as structurally incompatible with anonymity and informational self-determination, making individual "trimming" of provisions inadequate. For the dissent, the Money Bill route, centralised biometric database, and the risk of exclusion together mean that Aadhaar fails proportionality not merely at the level of specific sections but at the level of the scheme itself, leading him to invalidate the Act in its entirety.

Puttaswamy's debate on dignity, autonomy, and informational privacy offers the normative basis that both legitimises and constrains State use of digital infrastructures such as Aadhaar. When this approach is applied to Aadhaar, it highlights a fault line between a vision of privacy as a requirement for personality and freedom, and a more instrumental perspective that enables large-scale data systems to operate so long as specified protections are in place. The Aadhaar verdict therefore becomes a test case for whether Indian constitutionalism can legitimately arbitrate between welfare-oriented datafication and the requirement of informational self-determination.

DISCUSSIONS

Normative Foundations Deepened- Puttaswamy expressly relates privacy to human dignity, portraying it not as a luxury of the rich but as a requirement for real autonomy and the practice of other essential rights. The Court underlines that privacy protects the "inner zone" of the individual—choices concerning religion, affiliation, sexuality, and physical integrity—thereby rejecting prior assertions that socio-economically disadvantaged groups have lower privacy entitlements. This indicates a dramatic change away from the old "property or house-centred" view of privacy to an individual-centred, substantive definition that

[15] https://en.wikipedia.org/wiki/Puttaswamy_v._Union_of_India
[16] https://www.scobserver.in/cases/puttaswamy-v-union-of-india-fundamental-right-to-privacy-case-background/
[17] https://globalfreedomofexpression.columbia.edu/cases/puttaswamy-v-union-of-india-ii/
[18] https://ohrh.law.ox.ac.uk/defining-the-right-to-privacy-in-india-in-light-of-justice-ks-puttaswamy-anr-v-union-of-india-2017/

moves with the person rather than staying restricted to physical settings.[19]

Within this context, informational privacy is especially important for digital government. The Court understands that the State's ability to gather, aggregate, and analyze data provides it unparalleled control over people, possibly having chilling effects on dissent, association, and speech. Concepts such as the "right to be left alone" and "informational self-determination" are embraced or repeated, connecting Indian law with worldwide views that consider control over personal data as vital to dignity and freedom in networked society.

Puttaswamy also predicts downstream changes by relating privacy to equality and non-discrimination. Data-based profiling may repeat and reinforce existing social inequalities, especially when algorithms and databases include prejudices regarding caste, class, gender, or religion. By locating privacy at the crossroads of liberty and equality, the ruling provides the framework for future analysis of how digital identification and welfare technologies could deepen structural disadvantage even when officially neutral.

Applying These Principles to Aadhaar- When these normative obligations are brought into the Aadhaar dispute, the Court must tackle not simply isolated instances of data exploitation but the whole design of a centralized biometric identification system. The Aadhaar structure incorporates obligatory or quasi-compulsory registration, storage of biometrics and demographic data in a central database, and repeated authentication across numerous life domains, from welfare access to tax and telecommunications. In essence, such a system implicates informational self-determination: the individual's capacity to select who gathers, processes, and distributes their data, for what objectives, and subject to what protections.

The majority in Aadhaar reconciles this issue by evoking a weighing of "two facets of dignity": autonomy and informational privacy, on the one hand, and the dignity of living a life free from deprivation via efficient benefit delivery, on the other. It finds that for disadvantaged groups, the dignity obtained via dependable access to subsidies and benefits might justify the imposition of biometric identification, provided the data acquired are "minimal" and backed by procedural protections. On this perspective, Aadhaar's design is not inherently violative of privacy; it becomes legally dubious only if particular applications (e.g., private-sector

[19] Human Rights Watch. (2017). *India's Supreme Court Upholds Right to Privacy*.

authentication, over-long data retention) exceed what is essential for welfare and fiscal purposes. Justice Chandrachud's dissent beginning from the same normative underpinnings, brings them to a sharper conclusion. For him, informational self-determination and anonymity are crucial to dignity and freedom; a system that makes biometric identification a requirement for basic rights, and seeds that identity throughout databases, profoundly transforms the citizen-State relationship. The opposition underscores that since the State controls a single biometric key that unlocks numerous data silos, the danger of ubiquitous surveillance and profiling is inherent in the framework, regardless of guarantees concerning present usage. This structural emphasis separates the dissent's approach from the majority's, which tends to see Aadhaar as acceptable in principle but needing "surgical" changes at the level of individual sections.

Proportionality as Doctrinal Innovation- Puttaswamy's adoption of proportionality indicates a transition from a "culture of authority" to a "culture of justification", forcing the State to justify why intrusions into privacy are essential and reasonable. The test, as crystallised in later discussion, contains four elements: (1) a law that is not arbitrary; (2) a legitimate objective; (3) reasonable connection and necessity (least restrictive means); and (4) a tight balance between rights costs and public advantages. Some judgments also hint to a "compelling State interest" requirement for extremely invasive procedures, introducing features of rigorous scrutiny.

In Aadhaar, the proportionality test delivers *tangible privacy gains*. Section 57 is knocked down to preclude regular Aadhaar-based KYC in the private sector; wide data-retention and metadata rules are reduced; and required bank and mobile links are invalidated for lack of need and legal justification. These findings highlight how proportionality may be a potent weapon to prune the most severe types of data excess, particularly if State explanations are insufficient or non-existent.

At the same time, the test is used to *uphold the core* of Aadhaar—enrolment, centralised database, and mandatory use for subsidies and PAN—on the ground that these measures are rationally connected to legitimate aims and that the "minimal" nature of data collected, combined with statutory limits, suffices to preserve the essence of privacy. The majority's reasoning considers biometric enrollment as a necessary trade-off for welfare efficiency and tax enforcement, so defining privacy as a right that may be

constrained in pursuit of socio-economic justice.[20]

Limits of Proportionality for Digital Infrastructures- Scholars and campaigners have questioned whether proportionality, as traditionally used, is well-suited to evaluate infrastructure-level measures like Aadhaar. Proportionality tends to break down a program into separate measures and assess each against its declared purpose; yet digital identification systems are *architectures* that receive their power from connectivity, aggregation, and function-creep. Risks such as merging of data silos, re-purposing of data, and long-term security vulnerabilities are systemic and may not be fully reflected by comparing specific parts against urgent policy goals.

Justice Chandrachud's dissent echoes this view by interpreting Aadhaar as fundamentally incompatible with strong informational privacy. He interrogates not only the wording of the Act and regulations, but also implementation contracts and technological aspects, identifying vulnerabilities such as foreign control over source code and inadequate control over third-party access. For the dissent, proportionality must account for real-world evidence of authentication failures, data breaches, and exclusion, rather than depending mainly on State claims about security and little information. This approach needs a *thicker evidential basis* and a more cautious posture toward techno-optimistic promises, particularly when constitutional rights of disadvantaged groups are at issue.

Civil society assessments further contend that proportionality, if implemented deferentially, might legitimise large monitoring infrastructures by trimming only their most conspicuous excesses. In Aadhaar, although essential links and data-retention requirements were thrown down, the core premise—that every beneficiary and taxpayer might be subjected to biometric identification and ongoing authentication—remains intact. Given the irreversibility of biometric compromise and the difficulties of withdrawing or "opting out" of such systems, critics say that a more rigorous norm, closer to stringent scrutiny, should govern such designs.

Structural Criticisms vs. Formal Balance- The contradiction between *formal balancing and structural critique* is undoubtedly the core jurisprudential split in Aadhaar. The majority's method—identifying legitimate purposes, checking for reasonable linkage, and trimming out excessive provisions—preserves the State's digital-welfare initiative while expressing sensitivity to privacy. It

[20] Bhandari, V., et al. (2017). *An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict*. Indrastra Global.

indicates confidence that legislative and administrative fine-tuning, under judicial oversight, can address privacy threats without undermining fundamental infrastructures.

The dissent, by contrast, contends that some designs are *constitutionally suspect* independent of piecemeal alterations. When a single biometric identification is planted across banking, telecom, taxes, and welfare systems, the idea of de-anonymisation and thorough profiling ceases to be theoretical; it is baked into the architecture. From this standpoint, proportionality cannot be fulfilled by guarantees regarding present usage or by after-the-fact deletion regulations; it must investigate whether the fundamental structure of the system respects anonymity, self-determination, and the freedom to say "no" without abandoning essential rights.

This divide points to a broader challenge for constitutional law in the digital age: whether traditional tools like proportionality can adapt to evaluate *socio-technical systems,* or whether new doctrines and evidentiary standards are needed to grapple with algorithmic governance and data-driven power. Puttaswamy gives a rich normative vocabulary—dignity, autonomy, informational self-determination—but Aadhaar indicates that turning these ideals into effective limits on digital infrastructures remains an unfinished enterprise.[21]

Exclusion, Welfare, and the Paradox of Aadhaar- Aadhaar was established as a tool of inclusion—a system to equip every citizen of India with a valid digital identification that may enable access to key social services. The State justified its implementation as a constitutional pursuit of distributive justice: by ensuring that subsidies and services reached genuine beneficiaries, Aadhaar was said to embody the directive principles of equitable resource allocation and advance Article 21's guarantee of a dignified life. The Supreme Court's majority ruling essentially endorsed this logic, considering Aadhaar as a mechanism that operationalises social rights rather than harming personal freedoms. In doing so, it characterized Aadhaar not as an intrusion but as an empowering device—what it termed the "dignity of identity." [22]

However, field research, press reports, and civil-society investigations have repeatedly proven that Aadhaar's promise of inclusion coexists with worrisome patterns of exclusion. Biometric verification failures—due to mismatched fingerprints, worn fingerprints of manual laborers, inadequate internet connection, or gadget malfunction—have led to rejection of rations under the

[21] Bhandari, V., et al. (2017). *An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict*. Indrastra Global
[22] Drishti IAS. (2018). *Supreme Court Upholds Aadhaar's Constitutional Validity*.

Public Distribution System (PDS) or cessation of pension payments. Marginalised groups—daily-wage laborers, the elderly, individuals with disabilities, and rural women—face increased risks since they depend largely on welfare benefits and frequently lack digital literacy to understand Aadhaar's procedural intricacies. Thus, although Aadhaar was supposed to make the State more efficient, its technological mediation may change welfare from a right into a conditional privilege available only via successful electronic verification.

The majority ruling accepted the potential of such exclusions but regarded them as administrative quirks rather than fundamental flaws. The Court expressed confidence that enhanced infrastructure, grievance procedures, and stronger administration could remedy these flaws without invalidating the plan. This deferential posture reflects a conceptual choice: it lays the burden of remedy on implementation rather than on constitutional revision. Justice Chandrachud's dissent, by contrast, regarded exclusion as essential to Aadhaar's architecture—centralisation and need on ongoing verification made denial of rights an unavoidable, not accidental, conclusion.

The Paradox of Aadhaar—that a system meant to enfranchise the poor might worsen inequality—reflects a bigger global trend where digital welfare infrastructures risk converting individuals into data subjects whose presence in the public arena relies on algorithmic identification. Constitutional law generally defends against such reliance by highlighting rights as unconditional; however Aadhaar binds access to rights with technical compliance. Whenever the mechanism fails, dignity and autonomy are suspended.

The privacy verdict's ambition to maintain individual dignity, however, is inadequate unless privacy is accompanied with inclusion measures and accountability systems. This involves legislatively supported rights of appeal for authentication failure, independent audits of data correctness, and an enforceable "right to manual override" assuring that no individual is denied vital services for lack of biometric confirmation. True constitutional inclusion will depend not only on keeping a database but on guaranteeing that every digital identity corresponds to an empowered, rights-bearing individual capable of demanding entitlements without technical mediation failures.

Implications for Data Protection Law and Future Litigation- The recognition of informational privacy in Justice K.S. Puttaswamy v. Union of India (2017) represented the first explicit constitutional statement that the acquisition, storage, and broadcast of personal data may harm dignity and

liberty as directly as physical coercion or censorship. The Court's proposal for a comprehensive data protection system was both a remedy for existing shortcomings and a blueprint for legislative action. It requires the State to guarantee that digital governance, welfare delivery, and commercial data processing occur within a framework of consent, purpose limitation, and accountability. In this sense, Puttaswamy did more than announce rights: it constitutionalised the foundations of contemporary data protection.

The later Aadhaar ruling (2018) brought these concepts into the sphere of practice. By evaluating Aadhaar's architecture through the prism of proportionality, the Court demonstrated how privacy must work as both a negative right—protecting against arbitrary collection—and a positive obligation—compelling the State to create information systems that contain privacy by default. It accepted the legality of data-driven welfare but maintained that collecting must be constrained to statutory reasons, held securely, and safeguarded from profiling or function creep. Yet it also leaned significantly on executive promises, creating a gap between constitutional theory and practical detail. This strain made legislative follow-through imperative.

Legislative Trajectory Following Puttaswamy- The Supreme Court's privacy jurisprudence catalysed a variety of policy reactions. The Justice B.N. Srikrishna Committee (2018) produced the first comprehensive Personal Data Protection Bill, expressly recognizing Puttaswamy as its normative underpinning. The committee's report ("A Free and Fair Digital Economy") stressed fiduciary obligations of public and private data controllers, individual permission as the default legal basis for processing, rights of rectification and deletion, and constraints on cross-border data transfers. However, following iterations—the Personal Data Protection Bill (2019), the Data Protection Bill (2022), and the eventually passed Digital Personal Data Protection Act (DPDPA, 2023)—progressively reduced these protections. Broad State exclusions for "public order," "sovereignty," and "security of the State," combined with the lack of an independent and powerful Data Protection Board, prompted issues about whether the adopted framework genuinely honours the constitutional spirit of Puttaswamy.

The Aadhaar verdict so works as both precedent and warning. Its partial reliance to State assurances impacted a legislative approach that allowed wide government processing of personal data with minimal judicial supervision. Civil-society critiques—echoing Justice Chandrachud's Aadhaar dissent—argue that any data protection framework without sufficient constraints on government exemptions effectively inverts Puttaswamy: instead of

the State explaining restrictions, people must defend their privacy rights before the State. This inversion contradicts the dignity-centric understanding of privacy as a presumption in favor of autonomy.

Expanding Jurisprudence and Technological Frontiers- Future litigation will likely test how the Puttaswamy framework interacts with developing technologies—facial-recognition systems, predictive policing, algorithmic decision-making, and data-sharing under "Digital India" infrastructure. Already, High Courts have heard petitions challenging police use of crowd-monitoring cameras and state-managed facial-recognition databases without specific statutory justification. Petitioners typically reference Puttaswamy to claim that mass, suspicion-less monitoring breaches the legality and necessary standards of proportionality.

The following decade will find the Supreme Court challenged with challenges that transcend privacy beyond its basic analogue boundaries:

1. Whether biometric and demographic gathering using platforms like DigiYatra, National Digital Health Mission, and India Stack constitutes function creep;
2. How algorithmic profiling under welfare or credit-scoring schemes impacts equity and non-discrimination; and
3. To what extent automated decision systems must contain openness and human-review protections to maintain the right to be heard.

Each of these sectors ties its legal heritage to Puttaswamy's tripartite test and its stress that data acquisition must meet legality, legitimate intent, need, and proportionality.

Ongoing and potential review in Aadhaar Pending review petitions before the Supreme Court continue to contest central aspects of the Aadhaar verdict—particularly the majority's acceptance of the Act as a Money Bill, the adequacy of data-protection safeguards, and the proportionality analysis regarding financial and telecommunications linkages. If these reviews progress, they may give a chance to reset court criteria in light of six years of empirical experience, including authentication failures, exclusionary implications, and recorded data breaches. A more rigorous re-evaluation might either confirm the narrower view of Aadhaar as a benefit instrument or identify its inherent contradiction with the privacy values that inspired it.

Doctrinal Spill-Over: From Privacy to Digital Accountability- Beyond Aadhaar, Puttaswamy is transforming Indian

constitutional culture. The judgment's logic has already affected instances addressing phone tapping, social-media monitoring, Pegasus malware claims, and DNA-profiling laws. Lower courts often utilize Puttaswamy to require that government surveillance programs establish proportionality and acquire legislative approval. For instance, when adjudicating cyber-crime investigations or data-localisation requirements, courts now frequently assess whether collecting procedures are "least intrusive" and if persons are informed participants in digital ecosystems. This transition from power-based to justification-based governance constitutes one of the most fundamental legacies of the privacy ruling.

Toward a Rights-Based Data-Governance Future- Moving ahead, the task will be to transform Puttaswamy's dignitarian spirit into practical frameworks. Scholars recommend a multi-layered approach:

Constitutional entrenchment — reassert privacy as a non-derogable aspect of liberty, guaranteeing that emergency powers or national-security claims remain susceptible to court scrutiny.
Independent regulation - develop a fully independent data-protection body shielded from political interference, authorized to audit algorithms and give binding instructions.

Participatory governance - improve informational justice by incorporating citizen panels in technology design and data-government evaluation.

Judicial education and digital literacy — empower courts and law-enforcement agencies to grasp algorithmic technology while implementing proportionality standards.

Ultimately, Puttaswamy and Aadhaar combined create the framework for a "second-generation" constitutionalism of technology—one that not only restrains the State but also forces it to develop rights-respecting digital systems. Whether India's privacy jurisprudence grows into a globally relevant paradigm will depend on how future benches operationalise these concepts in situations well beyond Aadhaar: from smart cities and predictive policing to artificial intelligence and genetic databases.

The constitutional story that began with a retired judge's insistence on his right to privacy may thus evolve into a comprehensive legal architecture for India's digital century—if the courts and legislature honour Puttaswamy's guiding lesson: that human dignity is the first principle, and data must always serve

the citizen, never the reverse.[23]

CONCLUSION

The twin rulings in *Justice K.S. Puttaswamy v. Union of India (2017) and Puttaswamy (Aadhaar II) (2018)* combined constitute a watershed point in Indian constitutionalism. They reinterpreted the relationship between the person and the State in the digital era, positioning privacy as vital to human dignity, autonomy, and liberty under Article 21. By overruling M.P. Sharma and Kharak Singh, the Supreme Court addressed a long-standing doctrinal gap, upgrading privacy from a peripheral moral claim to a justiciable constitutional right. This shift established India among the few post-colonial nations to legally embed informational privacy within the wider architecture of basic rights.

Yet, the Aadhaar verdict demonstrates the difficulty of implementing these abstract concepts to a massive socio-technical system enmeshed in social policy. The majority endorsed the Aadhaar framework as a legal device for distributing benefits and limiting leakages, noting that it enhances distributive justice and the dignity of inclusion. However, it concurrently knocked down sections authorizing private-sector usage, over-broad data retention, and mandated links with banking and telecom services, therefore acknowledging privacy's restricting role even in assistance systems. Justice Chandrachud's dissent went further, characterizing Aadhaar as inherently incompatible with informational self-determination and warned that the centralised database paradigm risks transforming citizenship into conditional visibility before the State. The contrast between both approaches—incremental balancing vs structural incompatibility—defines the current constitutional debate on India's digital welfare architecture.

The larger effect of Puttaswamy is its normative reorientation of constitutional interpretation. It has adopted proportionality as the main standard for adjudicating rights limits, requiring the State to explain each incursion by legality, legitimacy, need, and balance. This approach now informs judicial assessment in domains well beyond Aadhaar: from surveillance and facial-recognition deployment to DNA profiling and online speech. The ruling also catalysed legislative solutions, propelling India's data-protection trajectory from the Srikrishna Committee proposal to the Digital Personal Data Protection Act 2023. However, the existence of extensive governmental exemptions and minimal institutional independence implies that the constitutional promise of Puttaswamy remains only partly

[23] http://www.manupatracademy.com/LegalPost/MANU_SC_1054_2018

realized.

Empirical realities, notably exclusion in welfare distribution, further illustrate the contradiction of Aadhaar: a system meant to empower the poor might, via authentication problems or infrastructure deficiencies, end up excluding those most reliant on State help. Unless privacy and inclusion are understood as mutually reinforcing rather than opposing principles, the dignity envisioned by the Court will remain incomplete. Constitutional faithfulness in the digital age needs not just rights on paper but also technology and governance systems that express such rights in reality.

Ultimately, Puttaswamy is less a static verdict than an evolving charter for India's digital future. It underlines that constitutional government must retain human dignity at its heart, even despite algorithmic efficiency and data-driven administration. The real test of these decisions will lay in whether India can design a data-governance framework that is both inventive, inclusive, and rights-preserving—one where technology advancement benefits the person, and not the other way around. If the State, Parliament, and court adopt this attitude, Puttaswamy will stand not only as a proclamation of privacy, but as a constitutional template for human dignity in the digital age.

REFERENCES

1. Bhandari, V., et al. (2017). *An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict*. Indrastra Global.ssoar
2. Columbia Global Freedom of Expression. (2023). *Puttaswamy v. Union of India (II)*.globalfreedomofexpression.columbia
3. Drishti IAS. (2018). *Supreme Court Upholds Aadhaar's Constitutional Validity*.drishtiias
4. Human Rights Watch. (2017). *India's Supreme Court Upholds Right to Privacy*.hrw
5. Oxford Human Rights Hub. (2017). *Defining the Right to Privacy in India in light of Justice K.S. Puttaswamy*.ohrh.law.ox
6. Supreme Court Observer. (2023). *Constitutionality of Aadhaar Act: Judgment Summary*.scobserver
7. Supreme Court Observer. (2025). *Fundamental Right to Privacy – Case Background (Puttaswamy)*.scobserver
8. Supreme Court Observer. (2025). *Aadhaar Review – Case Background*.scobserver
9. Taxolawgy. (n.d.). *What was the 2018 Supreme Court Ruling on Aadhar Card?* Justice for All.taxolawgy
10. Wikipedia. (2017). *Puttaswamy v. Union of India*.wikipedia