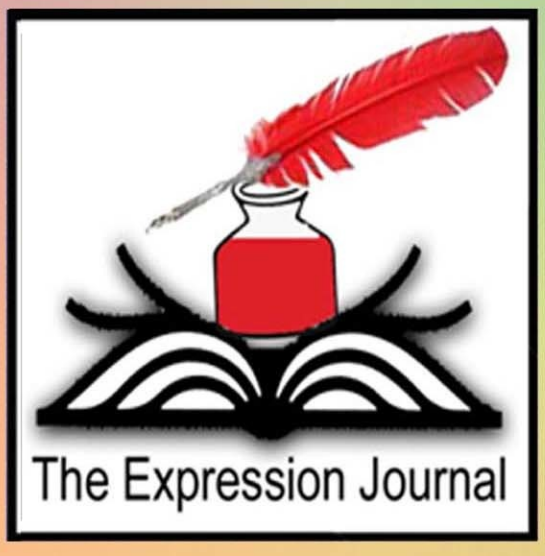
ISSN : 2395-4132

THE EXPRESSION

An International Multidisciplinary e-Journal

Bimonthly Refereed & Indexed Open Access e-Journal



Impact Factor 6.4

Vol. 11 Issue 4 August 2025

Editor-in-Chief : Dr. Bijender Singh

Email : editor@expressionjournal.com

www.expressionjournal.com

The Expression: An International Multidisciplinary e-Journal
(A Peer Reviewed and Indexed Journal with Impact Factor 6.4)
www.expressionjournal.com ISSN: 2395-4132

The Puttaswamy Judgment and its Impact on Privacy Jurisprudence in India

Mr. Anurag Suthar
Research Scholar
Faculty of Law, Tantia University, Sri Ganganagar
Dr. Atul Kumar Sahuwala
Research Supervisor
Faculty of Law, Tantia University, Sri Ganganagar

Abstract

The Constitution Bench decision of the Supreme Court in Justice K.S. Puttaswamy v. Union of India (2017) which held privacy as a fundamental right under the Indian Constitution set-in motion a transformative phase in constitutional interpretation and human rights jurisprudence. This paper seeks to trace the historical development leading to the emergence of the concept of privacy in India, critique the jurisprudence prior to Puttaswamy and the doctrinal inconsistencies that made it imperative for the Courts to clarify the constitutional principles. This paper analyses the reasoning of the nine-judge bench, which upholds privacy as a combination of dignity, autonomy and personal liberty, cementing its place as indispensable necessary for a progressive democratic community. The paper also discusses the judgment's far-ranging legal and policy impact - and how it has impacted data protection and government surveillance programmes, as well as state-driven schemes like Aadhaar. Through a comparative lens to other democratic regimes such as the United States, the United Kingdom, and the European Union, the paper also examines how privacy adjudication in India fares compared to global standards now. Taking a doctrinal and analytical stance, the paper submits that although the decision may be a constitutional watershed, the lack of clear legal and institutional structure continues to present obstacles in the realization of privacy rights in practice. The paper ends with a discussion of ways to reinforce legal protections, institutional accountability, and public education in the age of digital governance.

Keywords

Right to Privacy, Puttaswamy Judgment, Fundamental Rights, Data Protection, Surveillance, Constitutional Law, Digital Governance.

The Expression: An International Multidisciplinary e-Journal
(A Peer Reviewed and Indexed Journal with Impact Factor 6.4)
www.expressionjournal.com ISSN: 2395-4132

The Puttaswamy Judgment and its Impact on Privacy Jurisprudence in India

Mr. Anurag Suthar
Research Scholar
Faculty of Law, Tantia University, Sri Ganganagar
Dr. Atul Kumar Sahuwala
Research Supervisor
Faculty of Law, Tantia University, Sri Ganganagar

Introduction

The transformation of the right to privacy into a fundamental right by the Indian Supreme Court in Justice K.S. Puttaswamy v. Union of India (2017) marks a significant juncture in Indian constitutional history. Before this judgment, the privacy of Indian citizens was treated inconsistently by the nation's courts—a right that might be acknowledged here and there, but was never thoroughly affirmed as protected by the country's Constitution. The prior decisions in M.P. Sharma v. Satish Chandra (1954) and Kharak Singh v. State of Uttar Pradesh (1963) were based on a narrow and disjointed interpretation of privacy in consonance with the regime of rights as it existed then, which was a reflection of that time.[1] Due to limitations in the Constitution's text, which is silent on the issue of privacy, the right to privacy was neglected and the more widespread role of the state in economic and social matters gave the courts little space to assert the right of the individual to self-determination. The socio-legal terrain though changed irrevocably in the subsequent decades especially with the rise of the digital technologies, the rise of state sponsored biometric identification programs like Aadhaar, the increased datafication of citizenly identities and a new phase of legal consciousness about personal autonomy, informational control and dignity.

In so far as the latter is concerned, it also set right a breach of judicial inconsistencies and mapped out new architecture of fundamental rights under the Constitution. In a unanimous judgment, the Court emphasised that a citizen's right to privacy was not a derived or ancillary right but a right that itself was recognised as a fundamental right under the Constitution. It weaved privacy into the very texture of Articles 14, 19, and 21 and gave it the character of equality, liberty, and life. In so holding, the Court rendered privacy a normative and institutional cornerstone of

[1] Bhatia, Gautam, *The Transformative Constitution: A Radical Biography in Nine Acts*, HarperCollins India, 2019.

constitutional democracy, as the enabling right by which citizens are capable of exercising their civil and political liberties in a substantive way. The focus of the judgment on informational self-determination, decisional autonomy, and bodily integrity demonstrates a sophisticated, and forward-looking approach to personal rights in the digital age. The acknowledgment of privacy, not as one that merely protects against state intrusion, but as a substantive right rooted in human dignity, was a philosophy of judicial interpretation that moved constitutional liberty beyond the text to a more active and expansive conception.

The stakes of the judgment go well beyond doctrinal clarity. It has sent ripples through bills, executive moves, public policy discussions and civil society movements. The Supreme Court's definition of privacy as a precondition for democracy and personal choice has become the touchstone by which state surveillance programs, digital ID schemes and the legitimacy of data collection regimes are measured.[2] It has already defined judicial scrutiny for further cases relating to the Aadhaar scheme, social media regulation, and illegal surveillance during the investigation, and it continues to resonate in the lead-up to the Digital Personal Data Protection Act, 2023. The judgment therefore creates a constitutional yardstick against which the legitimacy of any infringement of privacy needs to be measured and that is by way of the test of legality, necessity and proportionality.[3]

But the post-Puttaswamy phase has highlighted serious deficiencies in the institutional implementation of this right. The courts provided the theoretical and right-based constitutional architecture now its implementation in terms of enforceable protections is inchoate. There is often a time lag and/or a watering down of legislative proposals with wide exemptions for state officials, creating suspicion over the sincerity and efficacy of implementation. The absence of a separate data protection authority for years; recurrent allegations of mass surveillance and electronic eavesdropping; and still limited public awareness about privacy rights – all have combined to undercut the ideal of the judgment. Moreover, at a time when private corporations have unprecedented access to personal information, the problem is bigger than the power of the state, and goes beyond regulation of data capitalism to also include ensuring that consent and transparency are meaningful.[4]

In this context, there is a pressing need not just to explore what the Puttaswamy decision held, but how it has influenced and catalysed the evolution of Indian privacy jurisprudence. As the nation manoeuvres around a more and more digitally oriented governance architecture and a data-fueled economy, the principles enshrined in Puttaswamy represent a legalistic guidepost and a democratic challenge. However, the respect with which these principles are honoured, institutionalised and developed will decide whether the right to privacy in India remains an illusion or grows into a truly actionable and enforceable truth.

---

[2] Sathe, S.P., *Judicial Activism in India: Transgressing Borders and Enforcing Limits*, Oxford University Press, 2002.
[3] Krishnaswamy, Sudhir, "Constitutional Morality and the Supreme Court: The Puttaswamy Case," (2018) 31(4) National Law School of India Review 1.
[4] Mehta, Pratap Bhanu, "The Inner Lives of Indian Citizens: Puttaswamy and Constitutional Identity," (2018) Seminar 707.

Objectives of the Study

This paper aims to:

- Trace the constitutional evolution of the right to privacy in India, culminating in the Puttaswamy judgment;
- Analyze the judicial reasoning and interpretative methods employed by the Supreme Court in establishing privacy as a fundamental right;
- Assess the legal and policy implications of the judgment, particularly with respect to surveillance, digital governance, and data protection;
- Explore the challenges that continue to obstruct the effective enforcement of privacy rights in India.

Methodology

The research methodology followed in this work is a doctrinal one, relying on primary sources of law (constitutional provisions, case law, and legislation). It is also comparative with respect to other jurisdictions, such as the United States, United Kingdom and the European Union. Secondary sources, such as articles of learned commentary, journal articles, policy papers, are also cited for analytical and contextual understanding of the legal nuances of the privacy jurisprudence in India.

Evolution of the Right to Privacy in Indian Constitutional Law

The Indian constitutional doctrine of privacy has followed a tortuous course, driven by variations in judicial perception, the transformation in social relations, and the increasing tension between the claims of the self and the demands of the state. Unlike a few constitutions which explicitly guarantee the right to privacy, the Indian Constitution is silent on the word. As a consequence, its recognition has been very much a judge-led project — tentatively first, but in the end radically — and in the meantime massively delayed.

The right to privacy was initially regarded with hostility by the Supreme Court in the early years of the constitutional regime. Here, in M.P Sharma v. Satish Chandra (1954) where the courts delved into the search and seizure provisions of the CrPC, it was pronounced that the Indian Constitution does not percolate privacy as one of the fundamental rights, in light with the Fourth Amendment of the US Constitution.[5] The Court emphasised their absence of textual support and devolved upon the state's questions of privacy in criminal law. Subsequently in Kharak Singh v. State of Uttar Pradesh (1963), the Court discussed the legality of police surveillance on crime-suspects.[6] Although it struck down nighttime home visits en masse, it declined to elevate privacy to a fundamental rights level. But remarkable as it may be, in his dissent in Kharak Singh, Justice Subba Rao had already sown the seeds for a radical reading of personal liberty by holding that privacy was part and parcel of ordered liberty under Article 21.

These narrow interpretations have been slowly but surely abandoned in the subsequent decades. In Gobind v. State of Madhya Pradesh (1975), the Supreme Court accepted rather reluctantly that privacy could be a fundamental right under Article 21, but did not make it a "cardinal" one.[7] Rather, the Court stressed that the right should crystallize in a society-specific manner, dependent upon societal conditions and

[5] *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300.
[6] *Kharak Singh v. State of U.P.*, AIR 1963 SC 1295.
[7] *Gobind v. State of M.P.*, (1975) 2 SCC 148.

legislative interests. Gobind was succeeded by Rajagopal v. State of Tamil Nadu (1994), where the Court categorically established the right to privacy as a constituent of the right to life and personal liberty. It stated that a citizen can protect his or her private life against the media or the state, unless the public interest determined otherwise.[8] At about this time, the case of People's Union for Civil Liberties (PUCL) v. Union of India (1997) also upheld privacy of telephonic conversations, demonstrating an emerging judicial trend to recognize information and communication privacy.[9]

Even after these advances, the legal status of privacy was ambiguous, because M.P. Sharma and Kharak Singh, as judgments of larger benches, were never formally overruled. This doctrinal contradiction reared its head in the litigation over the biometric Aadhaar identification scheme. The government had contended that privacy was not a constitutional right invoking M.P. Sharma and Kharak Singh as a binding precedent. To clarify this legal uncertainty, the Supreme Court formed a nine-judge bench in Justice K.S. Puttaswamy (Retd.) v. Union of India to finally answer the constitutional question.

The Puttaswamy judgement of 2017 definitively declared that the right to privacy is a fundamental right, which is contained within the right to freedom under Part III of the Constitution. The Court recognized that privacy is integral to human dignity and autonomy, including the freedom to make personal decisions, control one's personal information, and be free from overreaching interference by the state. Crucially, the court didn't take privacy to be one single, homogenous concept but acknowledged its many facets – privacy of the body, the autonomy to make decisions about oneself, and control over one's information – all of which were worthy of constitutional protection. The bench also rightly gave the go- by to the contrary conclusions in both M.P. Sharma and Kharak Singh, bringing privacy jurisprudence in line with changing democratic values.[10]

So, the trajectory of privacy in Indian constitutional law has travelled from a rejection and obscurity to doctrinal assertion and normative centrality. Recognition of privacy as a fundamental right is not a mere formality of words, instead it signifies a deep commitment to individual freedom, dignity, democratic freedom and an expression of commitment to human dignity. It is suggestive of the evolving role of the courts as the post-civil rights guarantor of freedom in an era of surveillance, big data and state intervention, basic dimensions of what it means to be both governed and to be a citizen. This development also intensifies the pressure on the state to prevent privacy from being invaded without good and lawful cause, and thus to subject arbitrary power to more effective control.

Case Name	Year	Judicial View on Privacy	Remarks
M.P. Sharma v. Satish Chandra	1954	Privacy not a fundamental right	Based on absence of explicit mention
Kharak Singh v. State of U.P.	1963	Majority: No right to privacy; Dissent: Privacy implied	First sign of evolving thinking
Gobind v. State of	1975	Conditional recognition under	Privacy not absolute

[8] *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632.
[9] *PUCL v. Union of India*, (1997) 1 SCC 301.
[10] Sathe, S.P., *Judicial Activism in India: Transgressing Borders and Enforcing Limits*, Oxford University Press, 2002.

M.P.		Article 21	
Rajagopal v. State of Tamil Nadu	1994	Clear recognition of privacy against media/state	Foreshadowed modern view
PUCL v. Union of India	1997	Right to telephonic privacy upheld	Emphasis on informational privacy
Puttaswamy v. Union of India	2017	Privacy recognized as a fundamental right	Landmark ruling

The table above depicts the incremental yet significant development of privacy jurisprudence in India. Since the approach of the Courts in M.P. Sharma (1954) and Kharak Singh (1963) was to either deny or doctrinally look at privacy in a limited sense, it is clear that the judicial approach in empirical terms was initially based on 'constitutional conservatism'. But as the Court confronted more sophisticated questions about personal freedom, it began tentatively to recognise privacy in cases such as Gobind (1975), without nevertheless conferring on it the full constitutional standing. In the 1990s with judgments like Rajagopal and PUCL, the judiciary started to inch towards treating privacy as a part of Article 21, especially in relation to media invasion and telephone tapping. These decisions formed the background for the full throated and wide recognition of privacy as a fundamental right in Puttaswamy (2017). The path reflects the transition from judicial reluctance to constitutional approval, and how societal changes and new technologies forced a wider interpretation of personal autonomy and informational control. The historical timeline also explains why the Puttaswamy ruling was indispensable—not just to usher in privacy as a fundamental right, but to settle decades of conflicting precedents and give doctrinal coherence.

Constitutional Interpretation of Privacy as a Fundamental Right

The Puttaswamy decision was a key doctrinal break in constitutional analysis of privacy, replacing a scattered judicial acknowledgment with a coherent, principle-driven affirmation of privacy as a fundamental right. What is novel in this judgment is the Court's attempt to situate privacy within the rubric of the broader constitutional conception of liberty, equality, and dignity, and not to treat privacy as a standalone entitlement. The judges looked at the textual provision purposively and founded on value, thereby rejecting literalistic interpretation and reiterated that core fundamental rights are not limited to what is enumerated; instead, they would expand to cope with the demands of the society.

At the heart of this change of interpretation was reading of privacy as an aspect of Article 21 (right to life and personal liberty).[11] The Court added that privacy is at the heart of individual freedom and individual autonomy, and that individuals make innumerable choices pertaining to the most important aspects of their lives- bodily, sexual, procreative, informational etc- without the interference of the state. In his lead opinion, Justice Chandrachud ruled that privacy is not an elitist preference but a core right for every person in a democratic society. "Privacy (he argued) blocks off the over-reaching arm of the state as well the exceeding arm of the society and offers resistance for both the negative obligations and the positive obligations of the state". [12]This

[11] Rao, M.S., "Fundamental Rights and the Right to Privacy: A Doctrinal Shift in Indian Constitutional Law," (2021) 43(3) Delhi Law Review 56.
[12] Shukla, V.N., *Constitution of India*, 13th ed., Eastern Book Company, 2020.

understanding aligned privacy with other civil liberties enshrined under Articles 14 and 19, and recognised that without privacy, the right to equality and the freedom of speech and expression would be rendered nugatory and impotent.

Puttaswamy also saw a dismantling of the Court's interpretative methodology. It expressly overruled M. P. Sharma and Kharak Singh to the extent they held or even implied that the status of privacy was not a fundamental right. These judgments in a different socio-political climate, were found to be in dissonance with both the current jurisprudence and constitutional morality. It then supplemented that with earlier judgments which had stepwise advanced privacy (like Gobind, Rajagopal and PUCL), evolved a coherent framework which brings coherence to decades of dispersed jurisprudence on privacy. In addition, the opinion expressly repudiated the concept that fundamental rights are to be strictly construed and instead held that the Constitution is an organic document, whose protections must receive a liberal construction in order to protect human dignity.[13]

A defining aspect of the opinion was the formulation of the three-part test of constitutionally valid restrictions on the right to privacy: legality, necessity, and proportionality. This test, drawn from and adapted to global constitutional practice — in particular European human rights jurisprudence — holds that any intrusion upon privacy must be prescribed by law; pursue a legitimate purpose; and be a proportionate means to that end. This proportionality structure imposes a real restraint on the state's intrusion into privacy, and strengthens the judiciary's function as an independent constitutional check on the legislative and the executive. Crucially, it also codifies a systematic approach for weighing individual liberties against the public good in contexts like surveillance, public health, and national security.

The judgment also referred to the tiered structure of privacy and classified three dimensions of privacy viz.(i) bodily or physical privacy -- which concerns the privacy of one's body, as well as the right to communicate and interact with others in private spheres; (ii) decisional privacy -- which concerns private intimate or personal choices; and (iii) informational privacy -- which concerns the privacy of personal data, the control that an individual can exercise over the dissemination of that data, and the control over his or her personal identity.[14] This multi-dimensional model is also able to provide better insight into how privacy plays a role in different aspects of our life, from personal relationships to online privacy behavior. Justice Kaul, in his separate opinion, stressed about the immediacy of data protection, and emphasised the need for a comprehensive data protection law to control the collection, storage and usage of such information. This study provided an input for discussions that eventually resulted in the Digital Personal Data Protection Act, 2023.

By characterising privacy as an essential precondition for the meaningful enjoyment of other basic rights, the Puttaswamy decision cemented it in the heart of Indian constitutionalism. It did more than provide declaratory relief and set out a normative framework that courts, legislators and administrators must now adhere to. In the process, it transformed privacy from a mere interest to a constitutional value,

[13] Singh, Mahendra Pal, "Human Dignity and Privacy in the Indian Constitution," (2018) 60(2) Journal of the Indian Law Institute 145.
[14] Ramaswamy, Shyamkrishna Balganesh, "Constitutional Interpretation and the Idea of Privacy in India," (2019) 12(1) Indian Journal of Constitutional Law 75.

recognizing that human dignity, autonomy, and freedom cannot be sacrificed at the altar of technological advancement or bureaucratic convenience. The decision embodies a new constitutional understanding: one that is great on individual agency and low on state power in an age when everything you do and say can be turned into evidence.

Implications of the Judgment on Policy and Governance

The Puttaswamy judgment has had wide-ranging consequences, doctrinally and structurally, in the anatomy of public policy and governance in India. In reading the right to privacy as a fundamental right, the Supreme Court put on the state a constitutional obligation to respect, protect, and promote the privacy of a person's life. This realization led to the reconsideration of the current legislation and administrative measures with respect to the collection, treatment and retention of personal data by the public authorities. The judgement itself acted as a direct and proximate challenge to Aadhaar, which was already under the scanner due to serious questions about surveillance, exclusion, and consent. Indeed, the requirement for a nine-judge bench itself came about as a response to questioning the constitutionality of Aadhaar, underscoring the belief that privacy was the fulcrum around which to measure the legitimacy of state sponsored digital identity schemes.[15]

In the post-Puttaswamy world, the coverage of any governmental behaviour touching upon privacy will now be determined by the threefold schools of "legality," "necessity" and "proportionality" as outlined in the judgment. This has dramatically changed the normative structure that shapes the exercise of state power. For instance, any biometric data, CCTV surveillance, mobile interception and even health data collection during pandemics need to stand this constitutional scrutiny. According to the court, no invasion of privacy can be justified unless it is supported by law, has a legitimate aim in the state and uses the least intrusive means to the aim. Practically speaking, this demand forces the legislative and executive branches to provide precise, tailored and fair procedures as well—vague or overly broad statutes may no longer survive constitutional scrutiny.[16]

The most prominent policy impact of the Puttaswamy decision is in its push toward a comprehensive legal regime for data protection. Justice Kaul, in his concurring opinion, came out in the open for the need of a holistic legislation aimed at safeguarding the informational privacy in the Information era. The government brought the Personal Data Protection Bill to address this judicial guidance in 2019 which was ultimately crystallised and emerged as the Digital Personal Data Protection Act, 2023. The Bill aims to set out norms for data processing, collection, consent, and the rights of data principals. It establishes a regulatory body to enforce the law as well.[17] It is the exemptions for the State and the potential watering down of the privacy guarantees established in Puttaswamy that have had the Act slammed by critics. The very fact that a data protection law came to be at all is an immediate fallout of the constitutional command of the Court.

---

[15] *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637

[16] Ramesh, R., "Privacy and Public Interest: Surveillance, Governance and the Indian State," (2020) 11(2) Indian Journal of Law and Technology 23.

[17] Doval, Shaista, "Between Puttaswamy and Practice: Governance Gaps in India's Privacy Regime," (2022) 5(1) Indian Constitutional Law Review 57.

Beneath the surface, the ruling also has created reverberations in several areas beyond data protection. The new guidelines also bring significant changes beyond the field of internal security and the armed forces to the surveillance of telephone lines, telephone prosecution and detention practices in criminal proceedings. Digital infrastructure (as well as service delivery mechanisms) for identity linked provision of services can no longer be blind to privacy and autonomy. In the field of health and education, two areas where sensitive personal data is common, the judgment has communicated a renewed focus on data minimisation, privacy and consent. More broadly on an administrative level, state actors would have to orient their possibly new rights-respecting dispositors in policy design and implementation, so that governance procedures do not become covert privacy violators for the sake of efficiency or the national interest.

Second, the decision has opened up a broader public debate over privacy as a democratic value and civic right. Civil society groups, legal scholars, and rights organizations have appealed to Puttaswamy, using the ruling to question opaque surveillance programmes, uncontrolled facial recognition projects, and the absence of transparency in the data being exchanged between the government and private organisations. So, the ruling has actually created an extra-judicial check on the state of not just courts but also citizens and watchdog institutions that can hold the state responsible for intrusions into private lives. In the process, it has been a factor in the emerging trend towards rights-based responses to techno-authoritarianism.

But despite establishing a strong normative base, the pragmatic effect on governance has been mixed. A variety of statutes and regulations still function in a manner contrary to privacy principles. The lack of a specialized privacy commission, delays in creating independent oversight agencies, and the state's growing hunger for surveillance technologies suggest a disconnect between mantras in the halls of justice and behavior in the halls of government. The proof of the pudding will be in whether or not Puttaswamy can change the practical routines of governance.[18]

Taken together, the Puttaswamy judgment has been both a spark and a choke in the Indian policy system. It has raised privacy to a constitutional value, affected legislative efforts, and redefined governance strategies. But its full potential still depends on continued legal reform, administrative commitment and judicial enforcement. As India digitalizes its public infrastructure and citizen interactions, the judgment stands as a constitutional guide to remind policy-makers that the upholding of personal dignity should be at the core of democratic governance.

Comparative Jurisprudence: Privacy Rights in Other Democracies

If the Puttaswamy decision is a significant turning point for privacy law in India, it can best be appreciated by locating it in the larger story of comparative constitutional development. Comparative law of democracies like the EU, US, and the UK provide valuable lessons about how privacy has developed across various legal traditions as well as institutionally protected. These differ in the degree to which privacy is recognized, the enforcement approaches, and the philosophical foundations for their legal frameworks.

[18] Khera, Reetika, "Aadhaar and the Challenge of Digital Governance," (2019) 54(10) Economic and Political Weekly 14.

In the EU has the GDPR, which treats privacy explicitly as such a fundamental right and arguably it offers the most rights-focused and the most comprehensive privacy framework. This right is guaranteed in Article 8 of the EU Charter of Fundamental Rights and is enforced by independent, robust data protection authorities in every member country.[19] The GDPR does not just defend the individual right to privacy; it reverses the burden of proof, and the responsibility on compliance, toward organizations handling personal data, thereby promoting individual empowerment and institutional responsibility.

The United States instead takes a patchwork-sectoral approach to privacy, a model based on market forces, not constitutional protections. While the US Supreme Court has identified a few privacy rights in relation to the Fourth Amendment (mainly, in the law of unreasonable search and seizure), there is no U.S. constitutional right to privacy. Federal regulations like HIPAA, COPPA, or the FCRA provide protections in certain sectors, but there's no overarching legal framework. Enforcement is largely through consumer protection practices and the Federal Trade Commission (FTC) rather than a dedicated agency for privacy.[20]

The United Kingdom, for example, has been shaped both by common law norms of confidence and privacy in tort, but also by the European model, known in relationship to the UK due to Brexit. The Human Rights Act, 1998 adopted the European Convention on Human Rights (ECHR), including Article 8, and further enshrined privacy rights in statutory form. The UK's Data Protection Act, 2018, implements and derogates the GDPR and is the relevant legislation post-Brexit, with some national variation.[21]

India's post-Puttaswamy framework, whilst in an evolving transition, models itself, on the one hand, on a constitutionally-based model; but one that, on the other, also must confront the shortcomings of both the American and European models — primarily, the question of state surveillance exemptions and lack of serious enforcement.

Comparative Framework: Privacy and Data Protection Across Jurisdictions

Aspect	**India (post-Puttaswamy)**	**European Union (GDPR)**	**United States**
Recognition of Privacy	Fundamental Right (Art. 21)	Fundamental Right (Charter Art. 8)	No general right; recognized in limited contexts
Legal Framework	Digital Personal Data Protection Act, 2023	General Data Protection Regulation (GDPR), 2018	Sectoral laws (e.g., HIPAA, COPPA, FCRA)
Enforcement Authority	Data Protection Board of India	Independent Data Protection Authorities	Federal Trade Commission (FTC); varies by sector
Scope of Consent	Consent-based, with wide exemptions for state	Explicit, informed, and freely given consent required	Often implied or embedded in terms-of-service
Limitations on	Public order,	Strict necessity and	National security

[19] General Data Protection Regulation (EU) 2016/679.
[20] Charter of Fundamental Rights of the European Union, 2000, Art. 7–8.
[21] *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

State	sovereignty, security exemptions	proportionality tests	exemptions broadly interpreted

The above table shows the different ways of addressing and protecting a right to privacy followed by leading legal systems. And yet India's constitution-based enshrinement of privacy brings closer to the European model in theory, but its implementation more closely resembles the American structure, including in key ways: most notably, the extensive latitude for state interests, still-nascent independent enforcement. The EU's regulatory framework is one of the most robust in the world, in terms of the protection of individuals and the security of the institutions serving them. The U.S. technology model, on the other hand, prizes innovation and free markets while often sacrificing personal data security. India, in the middle of these paradigms, has the predicament of implementing constitutional visions in a society and a politics which are ridden by the fear of surveillance, centralization, and digital illiteracy. The comparative jurisprudence is useful not only to put Puttaswamy in context, but also in identifying the direction for future legal reforms to establish a democracy that respects privacy.

Challenges and Criticisms of Post-Puttaswamy Jurisprudence

The Puttaswamy judgment, despite its doctrinal quality and progressive potency, has been subject to several significant road blocks. Though the Supreme Court declared the right to privacy to be a fundamental right in no uncertain terms and also crafted a structured framework to test its retreat, the transposition of the said principles in to the institutional domain has often been intermittent and half hearted. We are in the post-Puttaswamy era, where a disconnect between constitutional vision and legal application has exposed systemic, as well as normative deficiencies, in India's regime for privacy.

Perhaps the biggest challenge is the wide leeway given to the State under the Digital Personal Data Protection Act, 2023. While the Act originated in the wake of the Puttaswamy Court's recommendation that a statutory regime be brought in for data protection, it does not meet the constitutional goals enunciated in the decision. It also provides the central government with the power to exempt a government agency from the Act for reasons including national security, public order, and sovereignty (vague and open to broad interpretations). Such broad-based exceptions take away from the ratio and the mandate of the judgment emphasizing on the principle of legality and proportionality, and in the process, the constitutional substratum of informational privacy in cases involving the State.

Another major issue is there is no independent control mechanism. India has also created a Data Protection Board under the 2023 Act, but its composition and method of appointment cast a significant shadow over its independence and autonomy. Posed to belong to the purview of the executive, India's regulatory model is not an independent data protection authority like GDPR's. What is especially disconcerting is that the government of one of the countries that are rapidly increasing the scale of their surveillance technologies — facial recognition, predictive policing, and digital profiling — is a party to this campaign. No judicial or parliamentary controls over this practice that facilitates unbridled state intrusion, is congruent with the promises in Puttaswamy.

There is also growing state surveillance with inadequate legal safeguards – and these are areas where the spirit of the judgement seems to have been watered down. At present, the Indian Telegraph Act, 1885 and the Information Technology Act of 2000 (IT Act) still regulate interception, monitoring, and decryption, but without much

safeguard, process, or transparency. Despite the Puttaswamy Court's emphasis on the requirements of necessity and proportionality, surveillance operations are seldom submitted to substantive scrutiny by the judiciary, and individuals are frequently left with no means of redress. The non-transparent working of black boxes such as CMS and the absence of a holistic surveillance law demonstrates a massive shortcoming in harmonising state practices with constitutional norms.

Another critique relates to the Court's inadequate treatment of horizontal privacy breaches, involving particularly private actors and commercial companies. The ruling recognized that privacy is to be safeguarded against not only the State, but also in personal and digital relationships, yet the remedies against private intrusions, are in their infancy. In an era of digital commerce in which huge technology companies snap up and sell personal data as though it were real estate, such a chasm leaves people exposed. They are nothing more than "gates" that are buried away in long, impenetrable privacy policies, and people exercise little more than "ceremonial" control over their data as it passes into the business sector. The right to informational self-determination is therefore still more illusionary than real.

Further, the public ignorance and digital illiteracy have also undermined the practicality of the protection of privacy rights. Constitutionalism, however, could not function effectively regardless of how soundly worded, if there is not an active citizenry that participate in and are fully informed of it. Mostly people don't have a clue what is done with their data and can hardly fall back on an effective redress in case of abuse. This creates an asymmetry in which the institutional power, be it of the state or the corporations, is still more powerful than the individual rights.

Finally, it is the judiciary that comes in for criticism. While Puttaswamy may have paved the way for future privacy jurisprudence, the enforcement has been sporadic subsequently. For example, in the Aadhaar case, Puttaswamy (2018), the same court approved the Aadhaar programme, subject to certain conditions, by which the general impression was that of diluting the transformative character of the doctrine of Puttaswamy. Also, in other instances where digital freedoms have been at stake as issues, the Supreme Court has sometimes taken a deferent view of the executive and watered down the Puttaswamy standard.

Altogether, the post-Puttaswamy world is one of a constitutional ideal coming into conflict with policy. The decision stands as a landmark in establishing the normative roots of privacy, but how well that charted terrain is translated into reality is hampered by executive overreach, regulatory inertia, and absence of structural reform. For privacy to travel from the realm of paper to practice, the State will have to demonstrate real fidelity to rights-based governance while the judiciary must come to protect with vigour the values it once proclaimed so vigorously.

Conclusion and Suggestions

Justice K.S. Puttaswamy v. Union of India is widely hailed as a constitutional watershed, transforming the privacy rights calculus in India. With its endorsement of privacy as a fundamental right resting on the bedrock principles of dignity, autonomy, and liberty, the Supreme Court not only clarified longstanding doctrinal confusions but also reasserted the capacity of the Constitution to be an organic document that advances with the progress of science and changing moral demands. The judgment was a strong reassertion of individuals' rights in the age of increasing state power and

technological intrusions, especially in the era of digital governance, biometric data collection and mass surveillance. It has spread privacy from a vague idea to a right constitutionally enshrined with a framework of legal definition — legality, necessity and proportionality — over any interference.

But the post-Puttaswamy course of events shows that the constitutional recognition of a right does not necessarily imply that it would actually be protected in real terms. Legislative developments, such as the Digital Personal Data Protection Act, 2023, fall short of fully embodying the constitutional ethos enunciated by the court and tend to sanctify state's interests over individual autonomy. Institutional dependence, regulatory weaknesses, and persistent executive opacity in surveillance practices further highlight the precariousness of privacy protections in India. Whereas the opinion provided a normative roadmap whose potential is largely unrealised in the lack of strong statutory safeguards, administrative oversight and proactive role by civil society.

Several measures would be necessary to take the right to privacy from the judiciary's articulation to its effective practice. Exemptions provided to state agencies through data protection laws should be well-defined and subject to independent oversight in order to avoid sacrificing privacy in the name of the general interest. Secondly, it is necessary for the Data Protection Board to be sufficiently autonomous and endowed with actual enforcement skills including the audit, investigation and punishment of breaches. Third, India needs to enact a robust and transparent surveillance law that delimits the exercise of state powers and inscribes various procedural protections including a role for the judiciary and post facto accountability. Fourth, we have to learn how to build public knowledge around that, around what it means to be a digital citizen, how they can defend themselves and their constitutional rights. In the end, the courts must maintain vigilance in guarding the constitutional standards that they have developed and apply, particularly in an age where technological and bureaucratic structures that do circumvent individual consent may make such accountability more elusive.

Indeed, the Puttaswamy judgment is not an end point but a beginning—a structure which offers the ideal and the instruments for a privacy-respecting democracy. Its real test will not be the clarity of its language, but the robustness of the legal and institutional frames and the extent to which it gives individuals power to live in dignity, autonomy and freedom in the age of automation.