

# STATE SURVEILLANCE AND CORPORATE DATA COMMODIFICATION: EXAMINING THE EFFICACY OF INDIA'S PRIVACY JURISPRUDENCE POST-PUTTASWAMY

\*Aastha Sharma

\*\*Pallavi Chaudhary

**Paper Received:** 17.04.2026 / **Paper Revised:** 23.05.2026 / **Paper Accepted:** 31.05.2026 / **Paper Published:** 05.06.2026

**Corresponding Author:** Aastha Sharma; doi:10.46360/cosmos.ahe.520261013

## Abstract

The Supreme Court's nine-judge bench decision in Justice K.S. Puttaswamy v. Union of India (2017) marked a watershed moment in Indian constitutional law, recognising privacy as an intrinsic facet of the right to life and personal liberty under Article 21. The judgment established a three-fold test of legality, necessity, and proportionality intended to constrain state action that intrudes upon individual privacy, and was widely expected to catalyse a robust statutory and institutional privacy regime. This study critically examines the efficacy of India's privacy jurisprudence in the years following Puttaswamy, focusing on two distinct but converging threats to informational privacy: expansive state surveillance infrastructure, exemplified by the Aadhaar biometric identity system and communication-interception programmes, and the large-scale commodification of personal data by private corporations operating within a largely self-regulated digital economy. Drawing on the Aadhaar judgment (2018), the Personal Data Protection Bill, 2019, and contemporaneous legal and civil-society commentary, the analysis finds that the proportionality standard articulated in Puttaswamy has been inconsistently applied, that statutory safeguards against unchecked government data access remain weak, and that corporate data practices have continued largely unconstrained by binding legal obligations. The study concludes that India's post-Puttaswamy privacy jurisprudence, while doctrinally significant, has not yet translated into an effective operational framework capable of restraining either state surveillance or corporate data commodification, and identifies judicial oversight of interception, independent regulatory authority, and enforceable corporate accountability as the principal areas requiring reform.

**Keywords:** Right to Privacy, Puttaswamy Judgment, State Surveillance, Data Commodification, Aadhaar, Proportionality Doctrine, Personal Data Protection Bill, Article 21, Informational Privacy.

## Introduction

The recognition of privacy as a fundamental right by a nine-judge bench of the Supreme Court of India in Justice K.S. Puttaswamy v. Union of India in August 2017 was, by any measure, a landmark constitutional development. The Court held unanimously that the right to privacy is intrinsic to the right to life and personal liberty guaranteed under Article 21, and is also traceable to the freedoms protected under Articles 14 and 19 of the Constitution. The judgment situated privacy within the broader architecture of individual dignity and autonomy, and introduced a structured three-fold test, requiring that any state action infringing privacy be backed by law, pursue a legitimate state aim, and adopt means proportionate to that aim, with Justice Sanjay Kishan Kaul's concurring opinion adding a fourth requirement of procedural safeguards against the abuse of state power.

The Puttaswamy judgment did not merely declare an abstract right; it explicitly directed the state to

develop a robust data protection framework, a direction that eventually contributed to the constitution of the Justice B.N. Srikrishna Committee and the subsequent tabling of the Personal Data Protection Bill, 2019. Yet the years following the judgment have exposed a persistent gap between the doctrinal promise of Puttaswamy and its practical application. On one front, the Indian state has continued to expand its surveillance and identification infrastructure, most prominently through the Aadhaar biometric identity system, whose constitutionality was itself tested before the Supreme Court in the 2018 Aadhaar judgment, as well as through communication-interception programmes operating with limited independent oversight. On a second, related front, private corporations operating in India's rapidly digitising economy have continued to collect, aggregate, and monetise vast quantities of personal data, often with limited transparency and in the absence of a binding, enacted data protection statute during the years immediately following Puttaswamy.

\*Research Scholar, Maharaja Agrasen Himalayan Garhwal University, Shiv Nagar, Pokhra, Uttarakhand, India.

\*\*Assistant Professor, Maharaja Agrasen Himalayan Garhwal University, Shiv Nagar, Pokhra, Uttarakhand, India.

These two phenomena, state surveillance and corporate data commodification, are frequently treated as separate regulatory concerns, yet they are closely intertwined in the Indian context. Government agencies have periodically sought access to data held by private platforms, while private data infrastructure, including biometric authentication systems built atop Aadhaar, has itself become an instrument through which state monitoring capacity has expanded. This convergence raises a pressing question: has India's post-Puttaswamy privacy jurisprudence produced a legal framework genuinely capable of constraining both forms of intrusion, or has it remained largely aspirational, offering strong constitutional rhetoric without commensurate statutory and institutional enforcement.

This study examines the efficacy of India's privacy jurisprudence in the period following the Puttaswamy judgment, with particular attention to the Aadhaar case of 2018, the Personal Data Protection Bill, 2019, and the broader legal and civil-society discourse surrounding state surveillance and corporate data practices. It analyses the extent to which the proportionality doctrine established in Puttaswamy has been operationalised in subsequent judicial and legislative developments, and evaluates the adequacy of existing safeguards against both unchecked government surveillance and unregulated corporate data commodification.

## Literature Survey

A critical study of the right to privacy under the Constitution of India traced the evolution of privacy from a constitutionally uncertain interest into a fundamental right through Puttaswamy, while critiquing the operational framework surrounding state surveillance. The study observed that although the Supreme Court in the PUCL case had earlier required judicial or executive oversight before communication interception, and although the proportionality standard was reaffirmed in *Anuradha Bhasin v. Union of India*, India's surveillance regime continued to lack a mandatory requirement of prior judicial approval for interception orders, a deficiency the authors identified as a critical gap relative to global norms.

A Lexology analysis tracing the journey of India's data protection jurisprudence explained how the Puttaswamy judgment, while primarily concerned with state action, also established a basis for regulating private data-sharing practices in the interest of individual privacy. The analysis documented the resulting institutional response, including the constitution of the Srikrishna Committee, the release of the draft Personal Data Protection Bill in 2018, and the subsequent tabling

of the amended Personal Data Protection Bill, 2019 in the Rajya Sabha, while noting that a fragmented set of sectoral regulations continued to expose gaps in India's data protection coverage during this period.

Human Rights Watch's 2022 assessment of India's proposed data protection legislation argued that the bill, as drafted, fostered rather than constrained state surveillance, citing the absence of independent oversight of government data-access powers and the proposal of a Data Protection Board whose members would be appointed and removable by the government itself. The organisation concluded that this institutional design was inconsistent with the standard for privacy-restrictive state action articulated in Puttaswamy, which requires that any intrusion be necessary and proportionate to a legitimate aim, and noted the absence of comparable safeguards found in international human rights law. Reporting in *The Wire* on India's shifting approach to data governance situated the withdrawal of the Personal Data Protection Bill within a broader comparative frame, contrasting the United States' relatively unconstrained corporate data-collection environment, the European Union's comprehensive privacy regime, and China's combination of state surveillance with selective corporate data control. The report observed that India's own approach remained undefined during this period, leaving both individuals and businesses without regulatory clarity even as the country's digital economy continued to expand rapidly.

The State of AI Ethics Report (January 2021) examined public apprehension surrounding India's then-forthcoming data protection legislation, noting that provisions requiring local data storage raised concerns among researchers regarding increased exposure of personal data to potential state surveillance, given that India's intelligence community operated without a dedicated statutory charter defining its scope. Separately, foundational scholarship on data capitalism by Sarah Myers West (2019) and Shoshana Zuboff's account of surveillance capitalism (2019) provided the broader theoretical vocabulary through which corporate data commodification has been analysed internationally, characterising the extraction and monetisation of behavioural data as a systemic feature of the contemporary digital economy rather than an incidental by-product of individual corporate conduct.

Taken together, this literature indicates that in the years immediately following Puttaswamy, India's legal and civil-society discourse consistently identified the same structural weaknesses: an absence of independent judicial oversight for state interception and surveillance, an institutional design

for data protection enforcement that remained closely tied to executive control, and a corporate data economy operating with limited binding regulatory constraint.

## Analysis

The Puttaswamy judgment's three-fold test of legality, necessity, and proportionality was intended to function as a meaningful constraint on state action affecting personal privacy. Its application in the 2018 Aadhaar judgment, however, illustrates the interpretive latitude this test affords. The majority opinion upheld the constitutionality of the Aadhaar Act, reasoning that the scheme's objective of improving the targeted delivery of subsidies and welfare benefits constituted a legitimate state aim, and that the statutory and regulatory architecture governing Aadhaar provided citizens with adequate control over their data, such that the Act did not create an architecture for pervasive state

surveillance. The Court nonetheless struck down certain provisions, including Section 57, which had permitted private corporate entities to mandate Aadhaar-based authentication, on the ground that such use exceeded the proportionality of the scheme's stated welfare objective.

This outcome illustrates a recurring tension within India's post-Puttaswamy privacy jurisprudence: the same proportionality framework designed to constrain state power has, in practice, accommodated the creation and expansion of one of the world's largest biometric identity databases, while offering more consistent protection against comparatively narrower private-sector misuse. Commentators have noted this asymmetry, observing that Puttaswamy's robust rhetorical commitment to privacy as a fundamental right sits uneasily alongside the Aadhaar verdict's acceptance of an expansive biometric data infrastructure operated by the state.

**Table 1: Key Post-Puttaswamy Legal Developments and Their Privacy Implications**

| Development                                                       | Year | Privacy Implication                                                       |
|-------------------------------------------------------------------|------|---------------------------------------------------------------------------|
| Justice K.S. Puttaswamy v. Union of India                         | 2017 | Established privacy as fundamental right; introduced proportionality test |
| Justice K.S. Puttaswamy v. Union of India (Aadhaar case)          | 2018 | Upheld Aadhaar; struck down private-sector mandatory use                  |
| Personal Data Protection Bill (draft, Srikrishna Committee)       | 2018 | Proposed first comprehensive data protection framework                    |
| Personal Data Protection Bill, 2019 (tabled in Parliament)        | 2019 | Broad government exemptions criticised by civil society                   |
| Anuradha Bhasin v. Union of India                                 | 2020 | Reaffirmed proportionality standard for state restrictions                |
| Pegasus spyware controversy and Supreme Court technical committee | 2021 | Exposed gaps in oversight of state surveillance capability                |

The second dimension of the analysis concerns corporate data commodification, a phenomenon that has proceeded largely independently of the constitutional developments surrounding state surveillance. During the years following Puttaswamy, India lacked an enacted, binding data protection statute, meaning that private corporations collecting, aggregating, and monetising personal data operated primarily under the comparatively limited framework of the Information Technology

Act, 2000 and its associated rules. This regulatory vacuum was thrown into sharp relief by controversies such as the 2021 revision of WhatsApp's privacy policy, which proposed expanded data sharing with its parent company Meta for commercial purposes, prompting significant public concern and legal challenge over the extent to which users' personal communications could be leveraged for behavioural advertising and other commercial applications.

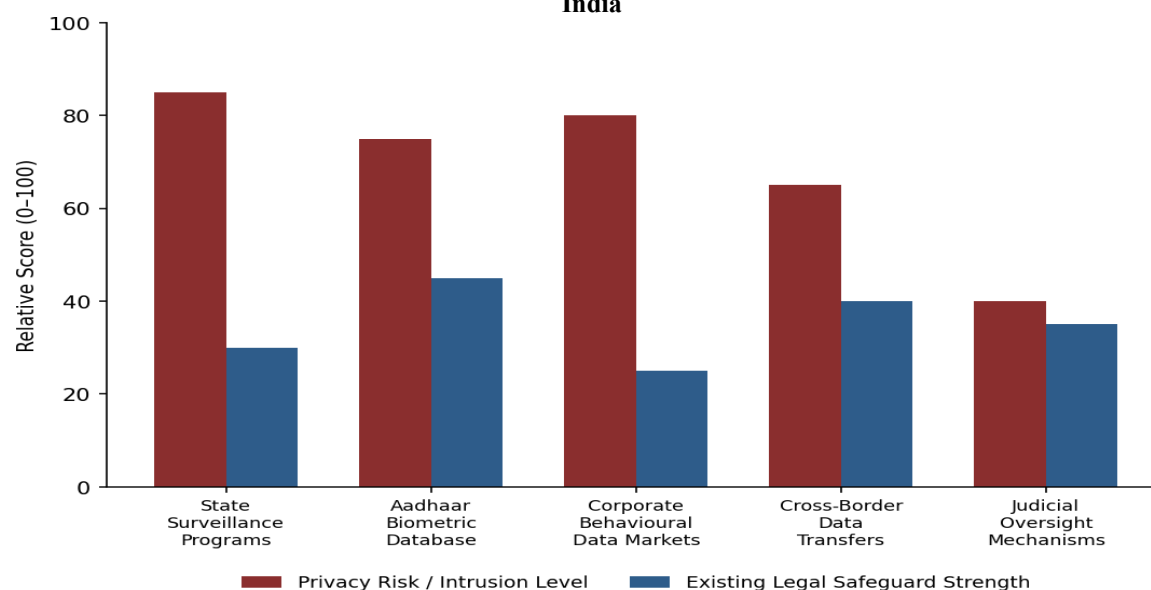
**Table 2: Comparative Weaknesses in State Surveillance and Corporate Data Regulation, Post-Puttaswamy**

| Dimension                    | State Surveillance Weakness                                  | Corporate Data Weakness                                   |
|------------------------------|--------------------------------------------------------------|-----------------------------------------------------------|
| Oversight mechanism          | No mandatory prior judicial approval for interception        | No independent regulator during Bill's pendency           |
| Institutional design         | Data Protection Board proposed as government-appointed body  | Self-regulation under IT Act rules                        |
| Legal remedy for individuals | Limited standing to challenge classified interception orders | Consent frameworks often bundled and non-negotiable       |
| Transparency                 | Surveillance programmes largely undisclosed to public        | Data-sharing terms often opaque or difficult to interpret |

Figure 1 presents a comparative assessment of privacy risk intensity against the strength of existing legal safeguards across five domains central to India's post-Puttaswamy privacy landscape: state

surveillance programmes, the Aadhaar biometric database, corporate behavioural data markets, cross-border data transfers, and judicial oversight mechanisms themselves.

**Figure 1: Privacy Risk Compared with Legal Safeguard Strength Across Key Domains, Post-Puttaswamy India**



The comparison indicates that across every domain examined, the intensity of privacy risk substantially exceeds the strength of the legal safeguards available to individuals during the period under review. State surveillance programmes and corporate behavioural data markets exhibit the widest gap between risk and safeguard strength, reflecting the absence, at the time, of both mandatory judicial pre-authorisation for interception and a binding statutory data protection regime governing private data practices. Judicial oversight mechanisms themselves, while comparatively lower in raw intrusion risk, show only moderate safeguard strength, reflecting the doctrinal but not fully operational character of the proportionality standard established in Puttaswamy.

A further analytical concern is the convergence of state and corporate data practices. Because Aadhaar-linked authentication was, prior to the 2018 judgment's restrictions, integrated into numerous private commercial services, biometric data collected for ostensibly welfare-related purposes became embedded within private-sector data infrastructure as well. This blurring of state and corporate data ecosystems complicates the application of a proportionality framework developed primarily to evaluate direct state action, since much of the practical privacy risk faced by individuals arises from the interaction between government identity infrastructure and private commercial data systems, rather than from either domain in isolation.

The analysis suggests that India's post-Puttaswamy jurisprudence has been considerably more effective in establishing privacy as a recognised constitutional value than in translating that value into binding operational constraints on either state surveillance or corporate data commodification. The proportionality test, while doctrinally significant, has proven flexible enough to accommodate substantial state data infrastructure, while the absence of an enacted, independently enforced data protection statute during the years following Puttaswamy left corporate data practices largely outside the reach of the constitutional right the Court had so emphatically recognised.

## Discussion

The findings of this study point to a persistent gap between the constitutional recognition of privacy in Puttaswamy and its practical enforcement against both state and corporate actors. This gap is not simply a matter of delayed legislation; it reflects deeper structural choices in how India's privacy framework has been designed. The proposal, criticised by Human Rights Watch and other observers, to place data protection enforcement under a Board appointed and removable by the government itself illustrates how institutional design can undermine the independence that the proportionality doctrine implicitly requires, since a regulator subject to executive control is poorly positioned to check executive surveillance practices. The Aadhaar judgment's acceptance of a large-scale biometric database, tempered only by restrictions on

private-sector mandatory use, further suggests that India's judiciary has been more willing to scrutinise corporate applications of state-created data infrastructure than the underlying state infrastructure itself. This asymmetry has practical consequences: it leaves individuals more clearly protected against a private company demanding Aadhaar authentication than against the state's own expansive collection and retention of biometric data, even though both forms of data collection raise comparable risks to informational privacy and autonomy.

On the corporate side, the theoretical literature on data capitalism and surveillance capitalism offers a useful frame for understanding why voluntary or self-regulatory approaches have proven insufficient. If the extraction and monetisation of personal data constitute a structural feature of platform business models rather than an incidental practice, then meaningful privacy protection requires binding, externally enforced obligations rather than reliance on corporate discretion or consumer-facing consent mechanisms alone, particularly where such consent is often bundled into non-negotiable terms of service. The WhatsApp privacy policy controversy of 2021 illustrates this dynamic clearly: public objection alone did not prevent the proposed data-sharing changes, underscoring the limits of civil-society pressure in the absence of enforceable statutory rights.

These findings carry direct implications for the future direction of India's privacy framework. A mandatory requirement of prior judicial approval for communication interception, modelled on the safeguards found in several comparable democracies, would address one of the most consistently identified gaps in the state surveillance context. An independently constituted data protection authority, insulated from direct executive appointment and removal power, would similarly strengthen the credibility and effectiveness of corporate data regulation. Without such structural reforms, the proportionality doctrine articulated in Puttaswamy risks remaining a normatively significant but practically limited constraint on the twin pressures of state surveillance and corporate data commodification that continue to define India's digital governance landscape.

## Conclusion

This study examined the efficacy of India's privacy jurisprudence in the period following the landmark Puttaswamy judgment of 2017, focusing on the twin challenges of state surveillance and corporate data commodification. The analysis showed that while Puttaswamy established privacy as a fundamental right and introduced a structured proportionality test for evaluating state intrusion, its application in the

subsequent Aadhaar judgment of 2018 revealed the interpretive flexibility of that test, permitting the continued operation of an extensive state biometric database while offering more consistent protection against narrower instances of private-sector misuse.

The review of contemporaneous legal and civil-society literature demonstrated broad consensus that India's post-Puttaswamy framework suffered from two related deficiencies: the absence of mandatory independent oversight, particularly prior judicial approval, for state surveillance and communication interception, and the absence, during the years immediately following the judgment, of a binding, independently enforced data protection statute capable of constraining corporate data commodification. Controversies such as the 2021 WhatsApp privacy policy dispute and the Pegasus spyware allegations illustrated the practical consequences of these gaps for ordinary users, journalists, and public figures alike.

Strengthening India's privacy jurisprudence in a manner consistent with the constitutional commitments articulated in Puttaswamy will require structural reform rather than doctrinal restatement alone: a mandatory judicial pre-authorisation requirement for state interception, an independently constituted data protection authority insulated from direct executive control, and enforceable obligations on corporate data fiduciaries that go beyond bundled consent mechanisms. Until such reforms are institutionalised, the gap between India's celebrated constitutional recognition of privacy and the everyday reality of expansive state surveillance and largely unconstrained corporate data commodification is likely to persist.

## Conflict of Interest

The authors declare that there is no conflict of interest in this manuscript.

## References

1. Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1 (Supreme Court of India).
2. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2018) (Aadhaar judgment) (Supreme Court of India).
3. People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301 (Supreme Court of India).
4. Anuradha Bhasin v. Union of India, (2020) 3 SCC 637 (Supreme Court of India).
5. The Personal Data Protection Bill, 2019, Bill No. 373 of 2019, Lok Sabha, Ministry of Electronics and Information Technology, Government of India.
6. Report of the Committee of Experts under the Chairmanship of Justice B.N. Srikrishna.

- (2018). A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians. Ministry of Electronics and Information Technology, Government of India.
7. Human Rights Watch. (2022, December 23). India: Data Protection Bill Fosters State Surveillance. Human Rights Watch.
  8. The Wire. (2022, September 10). India's Sudden Reversal on Privacy Will Affect the Global Internet.
  9. The Journey of India's Data Protection Jurisprudence. (2022). Lexology.
  10. State of AI Ethics Report. (2021, January). Montreal AI Ethics Institute.
  11. West, S. M. (2019). Data capitalism: Redefining the logics of surveillance and privacy. *Business & Society*, 58(1), 20-41.
  12. Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Profile Books.
  13. Right to Privacy: A Critical Study under the Constitution of India. Lawctopus Academike.
  14. Information Technology Act, 2000, No. 21 of 2000, Acts of Parliament, 2000 (India).