IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Privacy, Dignity, And Liberty: A Critical Examination Of The Puttaswamy Case

Lalitha M[1]
Dr. Seema Rajput[2].

Abstract

The Supreme Court's decision in *Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors.* (2017) represents a landmark in Indian constitutional law, affirming the right to privacy as a fundamental right under the Constitution. This article critically examines the ruling through the triadic lens of privacy, dignity, and liberty, highlighting its legal, philosophical, and policy implications. Central to the Court's reasoning is the adoption of the proportionality test, which serves as a judicial standard to assess the legitimacy and necessity of privacy infringements. The judgment's doctrinal clarity, normative reasoning, and transformative potential are assessed in light of both its promises and its limitations. Its influence is evident in subsequent rulings such as *Navtej Singh Johar* and *Joseph Shine*, where the Court extended privacy principles to areas of sexual autonomy and personal decision-making, signaling a broader constitutional shift towards individual liberty.

1. Introduction

The affirmation of the right to privacy as a fundamental right in the Puttaswamy judgment is among the most significant constitutional developments in India since the enactment of the Constitution. In a democracy where citizens are increasingly subject to state and corporate surveillance, the judgment reasserted the individual as the central subject of constitutional protection. It also marked a decisive departure from earlier jurisprudence that failed to recognize privacy as a right worthy of constitutional safeguarding.

2. Background and Procedural History

The case arose as part of a constitutional challenge to the Aadhaar scheme, which involved the compulsory collection of biometric and demographic data by the state. Petitioners, including retired Justice K.S. Puttaswamy, argued that Aadhaar violated the privacy rights of individuals by enabling intrusive state surveillance. The Union of India responded by citing older precedents such as M.P. Sharma v. Satish Chandra

[1] Lalitha M Research Scholar, Mansarovar Global University, Bhopal.
[2] Dr. Seema Rajput, Professor, Mansarovar Global University, Bhopal.

(1954) and Kharak Singh v. State of Uttar Pradesh (1962), where the Supreme Court had held that privacy was not a fundamental right.

3. Core Issues

The key issues before the Court were:

1) Whether the right to privacy is a fundamental right under Part III of the Constitution.

2) If so, what is the source, scope, and content of this right?

3) How privacy relates to other constitutional values such as dignity and liberty.

4. Legislations and framework

Article 21 — Protection of Life and Personal Liberty

Article 21 states that "No person shall be deprived of his life or personal liberty except according to procedure established by law." The Supreme Court, in *Puttaswamy*, interpreted the right to privacy as an intrinsic part of the right to life and personal liberty under Article 21. This means that privacy is fundamental to a dignified life and personal autonomy, making any infringement subject to strict judicial scrutiny.

Article 14 — Right to Equality

Article 14 guarantees equality before the law and equal protection of the laws. In the privacy context, Article 14 ensures that privacy rights are enforced uniformly without arbitrary discrimination. The Court emphasized that any state action infringing privacy must not be arbitrary and must satisfy reasonableness under Article 14, ensuring fair and equal treatment.

Article 19 — Protection of Certain Freedoms

Article 19 guarantees certain freedoms to citizens, including freedom of speech and expression (19(1)(a)), freedom of movement (19(1)(d)), and freedom to practice any profession (19(1)(g)), among others. The *Puttaswamy* judgment recognized that privacy is linked with these freedoms—especially informational privacy—which enables individuals to exercise their rights meaningfully without unwarranted intrusion or surveillance.

5. Critical Reflections

- ***Doctrinal Ambiguity***

While *Puttaswamy* affirms the right to privacy in sweeping terms, it does not provide a consistent taxonomy of privacy's multiple dimensions—namely, bodily privacy, informational privacy, and decisional autonomy. The plurality opinions invoke these aspects interchangeably without establishing clear doctrinal boundaries. As a result, subsequent courts and policy bodies have struggled to uniformly apply the ruling.

This ambiguity is particularly visible in the context of the Aadhaar scheme. Although the majority in *Puttaswamy (Aadhaar)* upheld the program's constitutional validity, it simultaneously struck down provisions permitting private sector access to biometric data, ostensibly on informational privacy grounds. However, the judgment stopped short of articulating how and why certain intrusions on informational privacy were constitutionally permissible while others were not, revealing a lack of doctrinal precision.

Lower courts have faced similar challenges. In cases involving digital surveillance, workplace data collection, or mandatory disclosure regimes (e.g., marital status or health conditions), the courts have often sidestepped a structured privacy analysis. This inconsistent application reflects the absence of a clear framework that categorizes privacy interests and aligns them with corresponding standards of review.

To address this ambiguity, scholars have proposed structured frameworks for conceptualizing privacy. Two particularly influential models are **Alan Westin's four states of privacy** and **Daniel Solove's taxonomy of privacy harms**.

Westin classifies privacy into:

1. **Solitude** – freedom from observation,
2. **Intimacy** – control over intimate relationships,
3. **Anonymity** – freedom to operate in public without identification, and
4. **Reserve** – control over the disclosure of personal facts.

Solove, on the other hand, categorizes privacy invasions into specific types of harms:

- **Information collection** (e.g., surveillance, interrogation)
- **Information processing** (e.g., aggregation, identification, secondary use)
- **Information dissemination** (e.g., disclosure, exposure, distortion)
- **Invasion** (e.g., intrusion into private life or decisional interference)

These frameworks could help clarify *Puttaswamy's* implications by distinguishing different kinds of privacy claims and aligning them with corresponding constitutional safeguards. For example:

- **Aadhaar's biometric data retention** primarily raises *informational privacy* concerns under Solove's "information processing" and "aggregation" harms.
- **LGBTQ+ rights**, as addressed in *Navtej Johar*, implicate *decisional privacy*, falling under Westin's "intimacy" and "reserve".

Integrating such a typology into Indian constitutional analysis would assist courts in applying *Puttaswamy* more consistently and transparently, especially when assessing proportionality under Article 21.

6. Comparative Perspectives on Privacy and Proportionality

The *Puttaswamy* judgment resonates with global constitutional jurisprudence, drawing parallels to landmark cases and regulatory frameworks that have shaped privacy law internationally. While *Puttaswamy* sets a foundational precedent for privacy rights in India, its limitations become clearer when viewed alongside international jurisprudence and regulatory frameworks.

- **United States:**

For instance, the U.S. Supreme Court's decision in *Griswold v. Connecticut* (1965) recognized privacy in decisional autonomy relating to intimate personal choices, a principle echoed in *Puttaswamy*'s emphasis on liberty and dignity. More recently, *Carpenter v. United States* (2018) extended privacy protections to digital data, requiring warrants for accessing cell phone location information, thereby reinforcing strict safeguards on informational privacy in the face of advancing technology underscored the evolving understanding of

informational privacy by holding that accessing historical cell-site location information requires a warrant, thereby affirming a heightened protection against digital surveillance.

These cases share *Puttaswamy's* emphasis on decisional autonomy and informational privacy, illustrating judicial recognition that privacy is not a fixed concept but one that adapts to technological and social changes.

- **European Union:**

In parallel, the European Union's General Data Protection Regulation (GDPR) exemplifies a comprehensive, rights-based approach to informational privacy, with principles such as lawfulness, transparency, data minimization, and explicit consent. GDPR's proportionality-oriented framework offers a rigorous template for balancing individual rights with public and commercial interests—a balance that Indian law has yet to fully achieve and data minimization reflect a nuanced application of proportionality, balancing individual rights against public and commercial interests.

By contrast, India's post-*Puttaswamy* legal landscape is still evolving to operationalize similar principles. While *Puttaswamy* lays down a proportionality test for privacy infringements, India's data protection statutes have yet to achieve GDPR's robustness or clarity, especially concerning enforcement and state exemptions.

These comparative insights illuminate the challenges India faces in translating *Puttaswamy*'s broad principles into a coherent, enforceable privacy regime. The absence of a dedicated and empowered data protection authority, coupled with legislative gaps and state exemptions, undercuts the effective realization of the right to privacy. Future reforms could benefit from adopting clearer typologies of privacy, strengthened enforcement mechanisms, and calibrated proportionality standards inspired by these global models.

Synthesis:

These international examples highlight the importance of a principled proportionality analysis and a clear categorization of privacy interests—lessons that *Puttaswamy* begins to embrace but has yet to fully internalize. A dialogue with these global frameworks could guide India's courts and legislature in refining privacy protections in the digital age.

7. Enforcement Challenges

A significant limitation of the *Puttaswamy* ruling lies in the practical enforcement of privacy rights. Until recently, India lacked a dedicated and autonomous Data Protection Authority (DPA), which is critical for overseeing compliance, investigating breaches, and adjudicating privacy complaints. The establishment of such an authority under the Digital Personal Data Protection Act, 2023 marks progress; however, concerns remain regarding its independence, powers, and effectiveness—particularly given the Act's broad exemptions for government agencies. Additionally, Indian courts have often demonstrated reluctance in granting strong injunctive or declaratory relief in privacy matters. Instead of proactively enforcing the right to privacy, lower courts have frequently adopted a cautious approach, deferring to the executive on issues of surveillance and data collection. This judicial hesitancy undermines the potential of *Puttaswamy* as a transformative tool for privacy protection, leaving individuals vulnerable to unchecked state and corporate intrusions.

- Practical enforcement mechanisms for privacy remain underdeveloped in India. Despite the Supreme Court's pronouncements, there has been a noticeable absence of a dedicated and independent data

protection authority to oversee privacy violations and adjudicate claims. The enactment of the Digital Personal Data Protection Act, 2023 marks progress but is criticized for granting overly broad exemptions to the state and lacking robust institutional checks.

- Furthermore, Indian courts have often struggled with applying *Puttaswamy*'s privacy principles consistently, particularly in emerging contexts such as digital surveillance, biometric data use, and mass state monitoring programs like CMS and NETRA. This judicial hesitancy, combined with legislative gaps, leaves privacy vulnerable to encroachments, undermining the transformative potential of the judgment.

- Robust enforcement mechanisms, including a fully empowered and impartial DPA, alongside proactive judicial intervention, are necessary to bridge the gap between the constitutional ideal and ground realities.

Moreover, courts have often been reluctant to issue clear, enforceable relief in privacy-related cases, especially those involving emerging technologies and surveillance. This gap limits the effective realization of privacy rights in day-to-day contexts

8. State Surveillance and Privacy Intrusions

While *Puttaswamy* robustly affirmed the constitutional right to privacy, it left unresolved critical questions regarding the legality and oversight of expansive state surveillance mechanisms such as the Central Monitoring System (CMS) and the Network Traffic Analysis (NETRA) program. These tools enable the interception, collection, and analysis of vast amounts of telecommunication and internet data, often without individualized suspicion or adequate judicial authorization.

Despite repeated concerns raised through Right to Information (RTI) queries and expert reports, the government has maintained a veil of secrecy around the operational details and legal basis for CMS and NETRA. Civil society organizations—including the Internet Freedom Foundation (IFF) and the Centre for Internet and Society (CIS)—have criticized these surveillance programs for their potential to violate informational privacy, chill free speech, and undermine democratic accountability.

For example, RTI disclosures have revealed that CMS has been operational since 2009, intercepting calls and messages centrally, but the protocols for authorization and safeguards against abuse remain largely opaque. Similarly, NETRA's capabilities to conduct large-scale network traffic analysis have been described as a "mass surveillance" tool lacking transparent oversight mechanisms.

These surveillance programs challenge *Puttaswamy's* proportionality framework, as their legal justifications and oversight structures do not consistently meet the requirements of legality, legitimate aim, and proportionality. Without judicial or parliamentary scrutiny, such intrusions risk becoming normalized, eroding privacy rights despite constitutional guarantees.

The Court and legislature must urgently address these gaps, imposing rigorous standards and transparent accountability mechanisms to align state surveillance practices with the constitutional right to privacy.

9. Impact and Subsequent Developments

- ***Legislative and Policy Responses***

The *Puttaswamy* judgment catalyzed significant legislative and policy discourse around privacy rights in India. Notably, it accelerated the drafting and eventual enactment of the Digital Personal Data Protection Act, 2023, which seeks to codify data protection principles grounded in the constitutional right to privacy. However, the Act has been criticized for granting wide-ranging exemptions to government agencies and lacking a fully independent Data Protection Authority, limiting its efficacy.

Additionally, the judgment influenced various government policies around biometric data usage, prompting amendments to Aadhaar regulations to bolster safeguards against misuse and unauthorized sharing.

10. Conclusion

Building upon the *Puttaswamy* framework, future reforms must address unresolved challenges. These include establishing a truly autonomous data protection authority with enforcement powers, legislating clear standards for government surveillance programs, and developing comprehensive frameworks distinguishing types of privacy harms as outlined in doctrinal typologies.

Future Directions and Recommendations

Building upon the *Puttaswamy* framework, future constitutional and legislative reforms must address the structural and normative gaps that continue to undermine the right to privacy in India.

- First, there is an urgent need to establish a **truly autonomous Data Protection Authority (DPA)** with adequate powers, independence, and accountability mechanisms. The current model under the Digital Personal Data Protection Act, 2023, falls short, as it allows significant executive control and lacks strong enforcement provisions. A restructured DPA, insulated from political influence, would ensure effective oversight and remedies for data breaches, wrongful processing, and misuse of personal information.

- Second, India must **legislate comprehensive standards governing state surveillance**. Mechanisms like the Central Monitoring System (CMS) and NETRA continue to operate without clear statutory mandates, judicial oversight, or transparency. Legislative intervention should mandate public accountability, judicial pre-authorization, and periodic audits, aligning surveillance practices with the *Puttaswamy* proportionality test.

- Third, the Court and policymakers should adopt **a nuanced framework for categorizing privacy harms**, distinguishing between bodily, informational, and decisional privacy. Drawing from scholarly typologies such as Daniel Solove's taxonomy or Alan Westin's classifications, such a framework would guide both adjudication and policy design, enabling context-specific safeguards and remedies.

- Fourth, **capacity-building in the judiciary and legal profession** is essential. Given the novelty and complexity of digital privacy issues, specialized training can help ensure consistent, informed, and rights-respecting jurisprudence across High Courts and tribunals.

- Finally, **future litigation** must strategically challenge practices and laws that fall short of *Puttaswamy*'s standards. Areas such as biometric profiling, algorithmic governance, and AI-driven surveillance represent new frontiers where constitutional principles must evolve and be tested. Civil society and legal practitioners must play a vigilant role in shaping this trajectory.

The *Puttaswamy* judgment laid the foundation for a constitutional culture of privacy rooted in dignity and liberty. The next phase requires translating that vision into actionable protections through institutional reform, legislative clarity, and sustained judicial engagement. Moreover, strategic litigation remains vital to expanding privacy protections, particularly in emerging domains such as artificial intelligence, health data, and digital identity systems. Robust judicial oversight and active civic engagement will be crucial in translating *Puttaswamy*'s constitutional vision into lived realities for all citizens.

Reference

1. M.P. Sharma v. Satish Chandra, AIR 1954 SC 300.
2. Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.
3. Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1.
4. Id., per Chandrachud, J., 298.
5. Francis Coralie Mullin v. Administrator, Union Territory of Delhi, (1981) 1 SCC 608.
6. Modern Dental College and Research Centre v. State of Madhya Pradesh, (2016) 7 SCC 353.
7. Navtej Singh Johar v. Union of India, (2018) 10 SCC 1.
8. Joseph Shine v. Union of India, (2019) 3 SCC 39.
9. Common Cause v. Union of India, (2018) 5 SCC 1.
10. Griswold v. Connecticut, 381 U.S. 479, 484–86 (1965)
11. Carpenter v. United States, 585 U.S. ___, 138 S. Ct. 2206, 2217–20 (2018)
12. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016 O.J. (L 119) 1.