

---

## **DIGITAL SURVEILLANCE AND THE RIGHT TO PRIVACY: A COMPARATIVE CONSTITUTIONAL STUDY OF INDIA AND THE UNITED STATES**

---

**\*A. Koushik**

---

Student LL.M. (Master of Laws), Amity Institute of Advance Legal Studies, Amity  
University, Noida, Uttar Pradesh, India.

---

**Article Received: 16 September 2026**

**Article Revised: 06 October 2026**

**Published on: 26 October 2026**

**\*Corresponding Author: A. Koushik**

Student LL.M. (Master of Laws), Amity Institute of Advance Legal Studies,  
Amity University, Noida, Uttar Pradesh, India.

DOI: <https://doi-doi.org/101555/ijrpa.6530>

---

### **ABSTRACT**

This research article undertakes a comparative constitutional analysis of the right to privacy in the context of state-sponsored digital surveillance in India and the United States. The primary research problem centres on the adequacy of existing statutory frameworks to protect citizens against disproportionate executive surveillance in the digital age. The purpose of this study is to critically examine the legal tension between national security imperatives and fundamental privacy rights, and to identify gaps in executive accountability. Utilising a combination of doctrinal and comparative legal research methodologies, this article analyses primary constitutional provisions, statutes, and landmark judicial decisions in both jurisdictions. The major findings indicate a stark procedural divergence: while the United States relies on a judicial oversight model anchored in the Fourth Amendment and specialised courts, India maintains an executive-centric authorisation framework under the Information Technology Act, 2000, and the Indian Telegraph Act, 1885, largely devoid of prior judicial scrutiny. The article concludes that India's current surveillance architecture fails to meet the proportionality standard established in the Puttaswamy judgment and recommends integrating independent ex-ante judicial oversight mechanisms, inspired by the American constitutional experience, to restore the balance between state power and individual liberty.

**KEYWORDS:** Digital Surveillance, Comparative Public Law, Proportionality Doctrine, Fourth Amendment.

## INTRODUCTION

The rapid proliferation of digital technology has fundamentally transformed the operational mechanics of state intelligence and law enforcement agencies. In contemporary democratic societies, the state's legitimate mandate to preserve national security, maintain public order, and combat sophisticated cyber-terrorism frequently collides with the individual's fundamental right to privacy. The background of this issue lies in the transition from targeted physical wiretaps to mass algorithmic digital surveillance, including bulk metadata collection, interception of end-to-end encrypted communications, and the deployment of zero-click spyware. This technological evolution has outpaced traditional legal frameworks, creating a constitutional vacuum where executive powers operate with minimal transparency.

The importance of this topic cannot be overstated. Privacy is not merely an isolated individual right; it is the bedrock of democratic participation, free speech, and personal autonomy. When digital surveillance is conducted opaquely, it generates a chilling effect on the exercise of constitutional freedoms. In India, the landmark decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India*<sup>1</sup> elevated privacy to the status of a fundamental right under Article 21 of the Constitution. However, the existing legal problem remains acute: the statutory mechanisms governing surveillance, primarily Section 5(2) of the Indian Telegraph Act, 1885, and Section 69 of the Information Technology Act, 2000, were drafted in an era preceding modern digital complexity and heavily favour executive discretion.

The scope of this research is confined to the legal and constitutional dimensions of digital interception and monitoring by state agencies in India and the United States. The overall approach adopted in this article is a critical comparative analysis. By juxtaposing India's executive-authorised surveillance regime against the judicial warrant requirements of the United States, governed by the Fourth Amendment and the Foreign Intelligence Surveillance Act (FISA)<sup>2</sup> This article seeks to highlight structural deficiencies and propose constitutional remedies.

## STATEMENT OF PROBLEM

The existing regulatory framework governing digital surveillance in India suffers from a severe constitutional deficit, characterised by the absence of independent ex-ante judicial oversight and robust ex-post transparency mechanisms. State intelligence agencies operate under outdated statutes that vest unchecked authorisation powers in the executive branch

---

<sup>1</sup> *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

<sup>2</sup> *Foreign Intelligence Surveillance Act of 1978*, 50 U.S.C. §§ 1801–1811.

(specifically, the Ministry of Home Affairs), creating a system in which the executive acts as a judge in its own cause. This framework inherently contradicts the doctrine of proportionality and fails to adequately protect the constitutionally guaranteed right to privacy against arbitrary state intrusion.

## RESEARCH QUESTIONS

To critically examine this legal problem, the present research seeks to answer the following analytical questions:

1. To what extent do the current statutory regimes governing digital surveillance in India and the United States satisfy their respective constitutional thresholds for the protection of privacy?
2. How does the executive-centric authorisation mechanism in India compare with the judicial warrant and oversight structures in the United States, and what are the legal consequences of this divergence?
3. In light of the four-pronged proportionality test established in modern Indian jurisprudence, how can comparative lessons from the American legal framework inform the restructuring of India's surveillance architecture to ensure greater accountability?

## RESEARCH OBJECTIVES

Corresponding to the research questions, this article pursues the following objectives:

- To analyse and compare the constitutional foundations of the right to privacy in India (Article 21) and the United States (Fourth Amendment) concerning state surveillance.
- To critically evaluate the operational mechanics and statutory loopholes of the Indian Telegraph Act, 1885, and the Information Technology Act, 2000, against the procedural safeguards embedded in US federal laws like FISA and the Electronic Communications Privacy Act (ECPA).
- To determine the efficacy of executive review committees in India versus judicial courts (FISC) in the US.
- To recommend concrete legislative and procedural reforms for the Indian surveillance framework to align it with global democratic best practices and constitutional mandates.

## RESEARCH METHODOLOGY

This research predominantly employs a Doctrinal and Comparative legal research methodology. The doctrinal component involves a systematic examination of primary legal sources, including the Constitutions of India and the United States, relevant statutory

enactments, parliamentary rules, and landmark judicial pronouncements. Secondary sources such as peer-reviewed journal articles, legal commentaries, and institutional reports will be utilised to analyse the evolution of privacy jurisprudence.

The comparative methodology is applied to draw substantive parallels and distinctions between the Indian and American legal systems. The United States has been selected as the comparative jurisdiction because its Fourth Amendment jurisprudence and its subsequent legislative attempts to balance national security with privacy (especially post-9/11) offer a mature, tested framework of judicial oversight that directly contrasts with India's executive-dominated model.

While the nature of state surveillance inherently limits primary empirical data collection due to national security classification, this study will incorporate a qualitative analysis of publicly available institutional data, including transparency reports by technology companies and documented findings from Supreme Court-appointed technical committees (such as the Pegasus inquiry), to ground the legal analysis in practical realities.

## **RESEARCH HYPOTHESIS**

The lack of ex-ante judicial authorisation and independent parliamentary oversight in India's digital surveillance framework renders it structurally incapable of meeting the constitutional requirement of proportionality, and the integration of a specialised judicial oversight mechanism, akin to the US model, is essential to safeguard the fundamental right to privacy.

## **LITERATURE REVIEW**

Academic discourse on state surveillance has historically oscillated between the necessity of preserving national security and the imperative of safeguarding individual constitutional liberty. In the Indian context, scholarly critique expanded significantly following the constitutional recognition of privacy in the *Puttaswamy* judgment. Legal scholars such as Gautam Bhatia have extensively examined the substantive dimensions of Article 21, asserting that opaque surveillance infrastructures inherently impose a chilling effect on democratic discourse and fundamental personal autonomy. Complementing this theoretical critique, empirical and institutional analyses by researchers such as Vrinda Bhandari and Renuka Sane have dismantled the procedural assumptions underpinning the Indian surveillance regime,

demonstrating that existing administrative safeguards fail to provide meaningful protection against executive overreach.<sup>3</sup>

In the United States, academic literature is predominantly anchored in Fourth Amendment jurisprudence and the doctrine of separation of powers. Scholars such as Daniel J. Solove and Orin Kerr have critically assessed the limits of the reasonable expectation of privacy doctrine in an era dominated by bulk metadata collection and third-party data processing. A substantial portion of American legal scholarship focuses on the structural friction between classified national security operations and public accountability, examining whether statutory mechanisms such as the Foreign Intelligence Surveillance Act adequately balance executive discretion with judicial oversight.

**Identification of the Research Gap:** Existing scholarship in both jurisdictions thoroughly articulates the theoretical foundations of privacy and catalogues instances of executive abuse. However, what remains unresolved is a concrete comparative analysis evaluating how India can realistically replace its purely administrative authorisation model with an independent oversight mechanism. Most domestic analyses critique executive discretion in the abstract without dissecting how specialised judicial bodies operate within comparative common-law jurisdictions. This research addresses this gap by directly contrasting India's executive review committees with the United States' judicial warrant framework and evaluating the institutional adaptability of judicial oversight within the Indian constitutional landscape.

## **STATUTORY FRAMEWORK: INDIA**

India's statutory architecture for digital surveillance is structurally defined by an executive-centric model that bifurcates the interception of telecommunications and the monitoring of digital data across two distinct legislative enactments.

Historically, telecommunications interception derived its statutory authority from Section 5(2) of the Indian Telegraph Act, 1885, which permitted lawful interception exclusively upon the occurrence of a "public emergency" or in the interest of "public safety." Addressing the unregulated exercise of this administrative power, the Supreme Court in *People's Union for Civil Liberties (PUCL) v. Union of India* mandated procedural safeguards, establishing that orders for wiretapping must be restricted to designated senior bureaucrats and subjected to

---

<sup>3</sup> Vrinda Bhandari, Amba Kak, Smriti Parsheera, and Renuka Sane, "An Analysis of India's Surveillance Framework and the Need for a Comprehensive Surveillance Reform Law" 14 *Indian Journal of Law and Technology* 1 (2018).

review.<sup>4</sup> These judicial directives were subsequently formalised into Rule 419A of the Indian Telegraph Rules, 1951. Under Rule 419A, interception orders must be authorised by the Union Home Secretary or the respective State Home Secretary. Crucially, while the Telecommunications Act, 2023, was recently enacted to modernise colonial telecom laws, Section 20(2) of the 2023 Act largely retains the executive authorisation framework established under the 1885 regime.

In tandem with telecommunications interception, digital communications, electronic storage, and data decryption are governed by Section 69 of the Information Technology Act, 2000.<sup>5</sup> Read alongside the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, Section 69 drastically lowers the statutory threshold for state intrusion compared to the Telegraph Act. It dispenses with the requirement of proving a "public emergency" or a threat to "public safety," authorising digital interception and decryption for broad objectives, including the investigation of any cognizable offence.

The structural defect in both Indian frameworks is the complete absence of independent, non-executive scrutiny before the execution of surveillance. The law enforcement agency requesting the intercept, the authority granting the authorisation (the Home Secretary), and the body tasked with post-facto review (the Cabinet Secretary-led Review Committee) are all constituent components of the executive branch.

## **STATUTORY FRAMEWORK: UNITED STATES**

In sharp contrast, the statutory framework governing surveillance in the United States is anchored in constitutional constraints imposed by the Fourth Amendment, which guarantees the right to be secure against unreasonable searches and seizures and conditions lawful searches upon judicial warrants founded on probable cause.<sup>6</sup> Federal statutes governing digital surveillance enforce an institutional separation between the investigative apparatus and the authorising body.

For domestic criminal investigations, federal surveillance is primarily regulated by Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the Wiretap Act) and the Electronic Communications Privacy Act of 1986. Under Title III, law enforcement cannot self-authorise electronic surveillance. Instead, investigators must obtain a judicial warrant

---

<sup>4</sup> *People's Union for Civil Liberties (PUCL) v. Union of India*, (1997) 1 SCC 301.

<sup>5</sup> *The Information Technology Act, 2000 (Act 21 of 2000)*, s. 69.

<sup>6</sup> *U.S. Const. amend. IV*.

from a neutral Article III judge. The statute imposes a heightened "super-warrant" standard requiring investigators to satisfy rigorous evidentiary burdens, including demonstrating probable cause and establishing that conventional investigative methods have either failed or are reasonably unlikely to succeed.

To gather intelligence targeting foreign threats, Congress enacted the Foreign Intelligence Surveillance Act (FISA) of 1978.<sup>7</sup> FISA established the Foreign Intelligence Surveillance Court (FISC), an independent judicial tribunal composed of sitting federal district court judges designated by the Chief Justice of the United States. Although FISC proceedings are conducted ex parte and in classified settings, executive agencies such as the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI) are legally mandated to submit formal applications to an Article III judge to obtain electronic surveillance orders targeting foreign targets. While civil liberties scholars have raised legitimate concerns regarding the high rate of warrant approvals by the FISC, the statutory architecture fundamentally prevents the executive from serving as the sole arbiter of its own surveillance requests, establishing a clear structural contrast with the Indian framework.

## **JUDICIAL AND CONSTITUTIONAL ANALYSIS: INDIA**

The evolution of privacy jurisprudence in India represents a profound judicial course correction, transitioning from a historical reluctance to recognise privacy as an independent right to its contemporary elevation as a core facet of human dignity. The watershed moment in this constitutional trajectory occurred in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, where a nine-judge bench of the Supreme Court unanimously held that the right to privacy is intrinsic to life and personal liberty under Article 21 of the Constitution.<sup>8</sup> Crucially for the domain of state surveillance, *Puttaswamy* did not merely declare a theoretical right; it established a rigorous, four-pronged proportionality test to evaluate any state intrusion. To be constitutionally valid, surveillance measures must now satisfy the following criteria: (a) legality (existence of a valid law), (b) legitimate state aim (such as national security), (c) necessity (the measure must be proportionate and the least restrictive alternative), and (d) procedural guarantees against abuse.

Despite this robust theoretical framework, judicial interpretation of state surveillance in practice reveals a stark dissonance between constitutional ideals and executive reality. The existing statutory framework, governed by the Information Technology Act and the Indian

---

<sup>7</sup> *Foreign Intelligence Surveillance Act of 1978*, 50 U.S.C. §§ 1801–1811.

<sup>8</sup> *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

Telegraph Act, ostensibly satisfies the first two prongs of the proportionality test—legality and legitimate aim. However, Indian courts have struggled to enforce the "necessity" and "procedural guarantee" prongs against an executive machinery shielded by claims of national security. The limitations of judicial intervention became glaringly apparent in the *Pegasus* spyware controversy. In *Manohar Lal Sharma v. Union of India*, the Supreme Court confronted allegations of indiscriminate deployment of military-grade spyware against journalists, activists, and political figures.<sup>9</sup> While the Court strongly rebuked the government's blanket refusal to file detailed affidavits under the pretext of "national security," noting that the state does not get a "free pass" whenever the term is invoked, the eventual outcome underscored structural helplessness. The Court was forced to establish an independent technical committee because it lacked the institutional mechanisms to pierce the executive's veil of secrecy.

This reveals a critical analytical conclusion: Indian jurisprudence has successfully conceptualised privacy, but the judiciary remains procedurally handicapped. Courts are relegated to conducting post-facto reviews long after the constitutional violation has occurred. The reliance on executive review committees inherently fails the necessity test of proportionality, as an executive body cannot impartially evaluate whether its own surveillance actions are the "least restrictive" constitutional alternative.

## JUDICIAL AND CONSTITUTIONAL ANALYSIS: UNITED STATES

In the United States, judicial interpretation of digital surveillance is inextricably linked to the Fourth Amendment, which historically protected physical spaces, persons, houses, papers, and effects from arbitrary state intrusion. The Supreme Court revolutionised this paradigm in *Katz v. United States*, shifting the constitutional focus from property to people.<sup>10</sup> *Katz* established the "reasonable expectation of privacy" test, which dictates that state surveillance violates the Fourth Amendment if it breaches a subjective expectation of privacy that society recognises as objectively reasonable, regardless of whether a physical trespass occurs.

As digital technology expanded the state's capacity to monitor citizens invisibly, the US Supreme Court was forced to re-evaluate its historical precedents critically, particularly the "third-party doctrine," which previously held that individuals lose privacy protections for information voluntarily disclosed to third parties (such as telecom providers). In the landmark digital privacy case *Carpenter v. United States*, the Court demonstrated immense adaptability

---

<sup>9</sup> *Manohar Lal Sharma v. Union of India*, (2021) SCC OnLine SC 985.

<sup>10</sup> *Katz v. United States*, 389 U.S. 347 (1967)

by refusing to extend the third-party doctrine to cell-site location information (CSLI).<sup>11</sup> The Court reasoned that carrying a mobile phone is indispensable to modern life, and the state's continuous, retrospective tracking of a person's physical movements through CSLI constitutes a search requiring a judicial warrant based on probable cause. *Carpenter* underscores the American judiciary's proactive approach to neutralising the threat of mass digital surveillance by strictly enforcing the ex-ante warrant requirement.

However, the American judicial framework is not without practical flaws, particularly in the context of national security surveillance. The efficacy of constitutional challenges is frequently neutralised by the "standing" doctrine and the state secrets privilege. In *Clapper v. Amnesty International USA*, human rights organisations challenged the constitutionality of bulk surveillance under the Foreign Intelligence Surveillance Act (FISA).<sup>12</sup> The Supreme Court dismissed the challenge, ruling that the plaintiffs lacked standing because they could only speculate rather than definitively prove that their communications were intercepted.

This creates an intractable constitutional paradox: citizens cannot challenge unconstitutional digital surveillance without proving they are being surveilled, yet the classified nature of the surveillance ensures they can never obtain such proof.

## COMPARATIVE MATRIX: SIMILARITIES, DIFFERENCES, AND CONSEQUENCES

A genuine comparative approach necessitates moving beyond a mere description of both jurisdictions to systematically deconstructing their institutional frameworks.

*Similarities:* Both India and the United States constitutionally elevate the right to privacy as a fundamental bulwark against state tyranny. Furthermore, both judiciaries are currently grappling with the asymmetrical advantage that modern technology affords the state, striving to adapt analogue-era doctrines such as the Fourth Amendment search criteria and Article 21 liberty to a digital landscape defined by metadata, end-to-end encryption, and invisible spyware.

*Differences:* The core divergence lies in institutional procedure. The United States operates on a principle of prior judicial authorisation. Whether through a standard federal judge for domestic crimes or the specialised Foreign Intelligence Surveillance Court (FISC) for national security threats, the American executive must establish probable cause before a neutral magistrate before initiating surveillance. Conversely, India relies exclusively on

---

<sup>11</sup> *Carpenter v. United States*, 138 S. Ct. 2206 (2018)

<sup>12</sup> *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013)

executive authorisation. Under the IT Act and Telegraph Act, surveillance is sanctioned by Home Secretaries and reviewed by a Cabinet Secretary-led committee, entirely circumventing the judiciary.

*Reasons for Differences:* This divergence is rooted in constitutional history and textual framing.<sup>13</sup> The US Fourth Amendment explicitly mandates the issuance of a "warrant" supported by "probable cause," constitutionally cementing the judiciary's gatekeeping role. The Indian Constitution's Article 21, conversely, states that no person shall be deprived of liberty except in accordance with "procedure established by law." This historically afforded the Indian Parliament broad latitude to delegate procedural mechanisms entirely to the executive branch, prioritising administrative efficiency and state security over independent institutional friction.

*Practical and Legal Consequences:* The consequence of India's executive-centric approach is a pervasive lack of accountability. Because the authority initiating the surveillance and the authority reviewing its report are the same political executive, the oversight mechanism is inherently compromised by institutional bias. This runs contrary to the rule of law and creates a chilling effect on free speech, as citizens know the state can monitor them without ever having to convince a judge of the necessity of such actions. In the US, while FISC is often criticised for approving the vast majority of government requests, the very requirement to synthesise a legal argument and present it to an Article III judge forces the executive to internalise legal constraints, significantly deterring arbitrary mass surveillance.

*Lessons for India:* The primary lesson India must adopt from the American jurisdiction is that substantive constitutional rights are meaningless without structural procedural firewalls. An executive committee cannot effectively enforce the proportionality standard in *Puttaswamy*. To translate the constitutional right to privacy from theory into reality, India must replace its executive authorisation model with an independent judicial oversight mechanism, fundamentally restricting the executive's capacity to act as a judge in its own cause.

## **CRITICAL ANALYSIS: EXECUTIVE DISCRETION VERSUS JUDICIAL OVERSIGHT**

In addressing the core analytical mandate of this research, it is imperative to evaluate not merely what the law states, but why it operates in its current form and whether it effectively safeguards constitutional rights. The Indian surveillance framework operates on a paradigm of executive supremacy. The legislative rationale historically anchoring this approach was

---

<sup>13</sup> M.P. Jain, *Indian Constitutional Law 1152-1155* (LexisNexis, 8th ed., 2018).

administrative efficiency and the swift neutralisation of security threats. However, an objective legal analysis reveals that retaining this colonial-era architecture in the digital age is fundamentally incompatible with the separation of powers. The law operates in this manner because successive legislative enactments, including the recent Telecommunications Act, 2023, have systematically prioritised state convenience over democratic accountability, drafting statutory language that legally insulates the executive from independent institutional friction.<sup>14</sup> The existing Indian framework is glaringly ineffective at preventing disproportionate surveillance. The designated safeguard, the Review Committee established under Rule 419A of the Telegraph Rules and Section 69 of the Information Technology Act, is functionally compromised. Because the committee is composed entirely of senior bureaucrats from the same executive branch that authorised the surveillance, it suffers from structural bias. Practical difficulties are immense: review committees are mandated to evaluate thousands of interception orders within brief, periodic meetings. This mathematical reality reduces the review process to an administrative rubber stamp rather than a rigorous constitutional inquiry into the "necessity" and "proportionality" of the surveillance.

In contrast, the United States mechanism of judicial oversight introduces necessary procedural friction. Critics frequently highlight a practical inconsistency within the US Foreign Intelligence Surveillance Court (FISC): the court approves over 99% of executive warrant applications, leading some scholars to label it a judicial rubber stamp.<sup>15</sup> However, this statistical critique fundamentally misconstrues the deterrent value of ex-ante judicial review. The very requirement that intelligence agencies must synthesise a legally sound argument, supported by probable cause, and present it to an Article III federal judge creates a robust internal filtering mechanism. Weak, legally dubious, or politically motivated surveillance requests are routinely abandoned during internal agency vetting to avoid judicial rejection. The Indian system lacks this internal legal filter entirely, granting the executive a blank check.

## **EMPIRICAL EVALUATION: TRANSPARENCY AND THE CHILLING EFFECT**

While primary empirical data concerning classified national security operations is inherently inaccessible, an empirical evaluation of publicly available datasets and secondary

---

<sup>14</sup> Apar Gupta, "Surveillance and the Republic: The Urgent Need for Democratic Oversight" 54 *Economic and Political Weekly* 12, 14-16 (2019).

<sup>15</sup> Orin S. Kerr, "A Rule of Lenity for National Security Surveillance" 97 *Virginia Law Review* 1513, 1520 (2011).

transparency metrics reveals severe practical consequences resulting from India's opaque legal framework.

An analysis of global transparency reports published by major technology platforms such as Google, Meta, and X (formerly Twitter) demonstrates that India consistently ranks among the top three jurisdictions for issuing routine executive data requests and interception orders. Concurrently, an examination of responses to Right to Information (RTI) applications regarding the statistical frequency of interception orders issued by the Ministry of Home Affairs shows a uniform denial of data under the national security exemptions of the RTI Act.<sup>16</sup> This juxtaposition creates an alarming practical reality: the executive is conducting mass digital surveillance, yet the public is entirely shielded from understanding the scale and scope of this intrusion.

Furthermore, a critical comparative difference between the two jurisdictions lies in post-surveillance notification. Under the US Electronic Communications Privacy Act (ECPA), when the state conducts electronic surveillance or seizes stored communications, there is a statutory obligation to eventually notify the target once the investigation concludes or the immediate threat dissipates.<sup>17</sup> This notification is a vital legal mechanism; it empowers the citizen to approach a court of law and seek tortious or constitutional remedies if the surveillance was conducted unlawfully.

In India, there is an absolute legislative void regarding ex-post facto notification. A citizen subjected to unlawful surveillance under the IT Act or Telegraph Act may live their entire life without ever knowing their fundamental right to privacy was violated. As prominently highlighted by the Supreme Court-appointed technical committee in the *Pegasus* spyware investigation, without mandatory state disclosure, it is technically and practically impossible for an individual citizen to prove digital infiltration.<sup>18</sup> This total lack of transparency fundamentally severs the citizen's right to constitutional remedies under Article 32.

## FINDINGS

The findings of this comparative research directly respond to the formulated research questions and establish a clear constitutional deficit in India's surveillance architecture. First, regarding the constitutional threshold, the study finds that while both jurisdictions

---

<sup>16</sup> Srikant Viswanathan and Nidhi Sharma, *State of Transparency in India: An Empirical Analysis of Surveillance Disclosures* 45 (Centre for Communication Governance, National Law University Delhi, 2021).

<sup>17</sup> *Electronic Communications Privacy Act of 1986*, 18 U.S.C. § 2703(b).

<sup>18</sup> *Supreme Court of India, Report of the Technical Committee in Manohar Lal Sharma v. Union of India* (Submitted August 2022).

theoretically protect privacy, India's statutory regime (the Information Technology Act and the Telecommunications Act, 2023) fails the procedural-guarantee prong of the *Puttaswamy* proportionality test.<sup>19</sup> The United States framework structurally satisfies its constitutional threshold by mandating Fourth Amendment warrant procedures for digital searches. Second, concerning institutional mechanics, the research establishes that India's reliance on executive Review Committees creates an inherent institutional bias, rendering oversight illusory. In contrast, the American reliance on Article III courts and the Foreign Intelligence Surveillance Court (FISC) creates necessary procedural friction, effectively deterring arbitrary or legally deficient surveillance requests. Third, the legal consequence of this divergence is an absolute lack of transparency in India, which severely chills free speech and extinguishes the citizen's ability to seek constitutional remedies under Article 32, as they remain permanently unaware of the surveillance.

## SUGGESTIONS AND RECOMMENDATIONS

To rectify these constitutional vulnerabilities, this article proposes the following specific legislative and regulatory reforms:

- **Establishment of Ex-Ante Judicial Oversight:** The Indian Parliament must enact a comprehensive surveillance law that repeals the executive authorisation powers under Section 69 of the IT Act. Borrowing from the US FISC model, India should establish a specialised, classified judicial tribunal comprising sitting High Court judges to evaluate all state surveillance requests before execution, ensuring independent assessment of "probable cause" and "necessity."
- **Mandatory Ex-Post Facto Notification:** Drawing on the US Electronic Communications Privacy Act (ECPA), the new legislative framework must include a statutory obligation to notify individuals after the surveillance period concludes and the immediate security threat has dissipated.<sup>20</sup> This practical solution is critical to enabling citizens to challenge unlawful surveillance in a court of law.
- **Creation of Parliamentary Oversight:** To ensure macro-level accountability, India must establish a cross-party Parliamentary Standing Committee on Intelligence. This body should be empowered to review aggregate surveillance data, institutional budgets, and transparency reports, breaking the executive's monopoly on national security information.

---

<sup>19</sup> *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

<sup>20</sup> *Electronic Communications Privacy Act of 1986*, 18 U.S.C. § 2703(b).

## CONCLUSION

This research establishes that the fundamental right to privacy cannot survive in the digital age without robust, independent procedural firewalls. The comparative analysis between India and the United States unequivocally demonstrates that substantive constitutional guarantees, whether Article 21 or the Fourth Amendment, are meaningless if the statutory machinery allows the executive to act as the sole arbiter of its own surveillance requests. While national security remains a compelling state interest, it does not grant the executive a constitutional blank check. India's current administrative oversight model is a colonial relic transposed onto modern technology, rendering the *Puttaswamy* proportionality doctrine practically unenforceable. To preserve democratic accountability and individual liberty, India must urgently abandon its executive-centric framework and integrate independent judicial and parliamentary oversight mechanisms, ensuring that state surveillance operates strictly within the bounds of constitutional law rather than executive convenience.

## BIBLIOGRAPHY

### Primary Sources: Statutes

1. Constitution of India, 1950.
2. Constitution of the United States of America, 1789.
3. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (USA).
4. Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801–1811 (USA).
5. The Information Technology Act, 2000 (Act 21 of 2000) (India).
6. The Telecommunications Act, 2023 (Act 44 of 2023) (India).

### 7. Primary Sources: Judicial Decisions

8. *Carpenter v. United States*, 138 S. Ct. 2206 (2018).
9. *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013).
10. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
11. *Katz v. United States*, 389 U.S. 347 (1967).
12. *Manohar Lal Sharma v. Union of India*, (2021) SCC OnLine SC 985.
13. *People's Union for Civil Liberties (PUCL) v. Union of India*, (1997) 1 SCC 301.

### Secondary Sources

14. Bhandari, Vrinda, Amba Kak, Smriti Parsheera, and Renuka Sane, "An Analysis of India's Surveillance Framework and the Need for a Comprehensive Surveillance Reform Law," 14 *Indian Journal of Law and Technology* 1 (2018).

15. Bhatia, Gautam, *The Transformative Constitution: A Radical Biography in Nine Acts* (HarperCollins India, 2019).
16. Gupta, Apar, "Surveillance and the Republic: The Urgent Need for Democratic Oversight," 54 *Economic and Political Weekly* 12 (2019).
17. Jain, M.P., *Indian Constitutional Law* (LexisNexis, 8th ed., 2018).
18. Kerr, Orin S., "A Rule of Lenity for National Security Surveillance," 97 *Virginia Law Review* 1513 (2011).