WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Surveillance and Privacy: The Threat to Individual Freedoms in the Name of Security in India

Faizan Alam**, Dr. Ujjwal Kumar Singh**

Law College Dehradun

ABSTRACT :

This encompassing analysis juxtaposes the state surveillance mechanism against individuals' rights to privacy specifically in India, weighing constitutional freedoms. The work scrutinizes the statutes authorizing surveillance, notably the Indian Telegraph Act of 1885 and the Information Technology Act of 2000, and describes how their imprecise definitions and absence of parliamentary or judicial review facilitate needless encroachment of executive power. By referring to important decisions like K.S. Puttaswamy v. Union of India and People's Union for Civil Liberties v. Union of India, this work examines how the evolution of privacy has become an avenue for constitutionally declared rights to constantly require the criteria of legality, necessity, and proportionality for any form of state intrusion. The actual cases of misuse include Pegasus spyware and Niira Radia tapes, showcasing an infringement on free speech and association and press freedom. By comparing these regimes with international models like U.S. FISA or EU GDPR, the paper highlights the glaring deficiencies in the areas of transparency and accountability. Recommendations include substantive reforms to the law, a requirement for court authorization prior to any surveillance being conducted, the appointment of independent oversight mechanisms, and improvements in data handling in line with constitutional requirements. The results of the research suggest that while surveillance is paramount for national security, its arbitrary enforcement is equally pregnant with threat to democratic freedoms, and this situation calls for the immediate recalibration of the legal and institutional structure toward the protection of privacy in a digitally changing environment.

Keywords: Surveillance, Privacy, Indian Constitution, Information Technology Act, Pegasus Spyware, Digital Rights

Introduction

Surveillance means systematic observation of an individual's behavior, communication, or activities usually by the government to protect state interests. In India, it is an essential weapon to neutralize threats to national security, such as terrorism and cybercrime, to help preserve some governmental order in the society. This practice, nevertheless, quite often comes in conflict with the right to privacy, a fundamental right intimately connected with personal liberty and autonomy. Such tensions arise from the surveillance legislation that empowers the state broadly to protect individuals while encroaching upon freedoms to speak, associate, and enjoy privacy. This dispute finds its roots in the legal framework of India, which accords sufficient power to intercept communications on grounds of security. However, the inadequacy of stringent safeguards raises alarms with respect to excesses where safety concerns may undercut the very rights that it intends to protect. The recognition of privacy as an intrinsic part of constitutional guarantees by the judiciary has only added fire to such arguments because these doubts raise the question: Do the surveillance mechanisms now operational conform to democratic tenets? This article portrays the delicate balance created by the Indian Telegraph Act and Information Technology Act permitting surveillance, while the case of *K.S. Puttaswamy v. Union of India*[1] reinforces the sanctity of privacy. The article addresses situations on the ground, such as the Pegasus spyware scandal, which utilized surveillance not only on journalists but also on human rights defenders, thus chilling free expression and exposing glaring procedural gaps. An examination of statutes such as Section 5(2) of the Telegraph Act and Section 69 of the IT Act, together with decisions including *People*'s *Union for Civil Liberties v. Union of India*[2], indicates the strong need for reform. The intent is explicit: to measure how surveillance acts as a productive evil to human freedoms if left unchecked, calling for a framework that reconciles the two. Contrasting India with the global perspective on this issue, the USA's FISA or the EU's GDPR reveals significant lapses in oversight and transparency that warrant a review of the existing modalities. The review introduces the further goes into a detailed examination comprising the legal infrastructure, the case law perspectives, and the real-world implications to build a case for a surveillance regime that honors the tenets of the Constitution while working towards security needs.[3]

* Student, B.A. LL.B. (Hons.), Law College Dehradun, Uttaranchal University, Dehradun, Uttarakhand, India.

** Assistant Professor, Law College Dehradun, Uttaranchal University, Dehradun, Uttarakhand, India.

[1] (2017) 10 SCC 1,.

[2] (1996) 9 SCC 367.

[3] State Surveillance vs Privacy in India: Legal and Constitutional Perspectives, *available at:* https://www.ipandlegalfilings.com/state-surveillance-vs-privacy-in-india-legal-and-constitutional-perspectives (last visited on March 14, 2025).

Legal Framework for Surveillance in India

A mixture of legislation from the colonial times, modern-day digital laws, and constitutional principles shapes India's regime of surveillance. This framework was intended to empower the state for monitoring communications under certain conditions, but it leaves some questions about privacy, transparency, and accountability. Though in the name of public safety or national security, different aspects of surveillance in India are mostly ungoverned through singular, comprehensive law or acts. Almost every aspect of surveillance is scattered across different provisions and rules in multiple statutes. The lack of a consolidated submission does create gaps in scope and enforcement and triggers friction between the state and the individual towards the Constitution.[4]

Indian Telegraph Act, 1885

The Indian Telegraph Act of 1885 is the most basic legal foundation for surveillance in India, which applies mainly to wired and wireless communications, including telephone conversations. Section 5(2) grants the Central or State government the power to tap or detain messages during a public emergency or where public safety is involved, if recorded reasons are given in writing. The provision is meant to meet immediate threats such as rioting or aggression from outside the country and so that the state can quickly enforce law and order. Rule 419A under the Act was framed after judicial intervention in *People*'s *Union for Civil Liberties v. Union of India*[5] to provide procedural safeguards for regulation of this power. Interception orders are to be issued only by officers not below the rank of Joint Secretary and are to be reviewed within seven days by a committee; such orders would cease within a maximum period of six months unless evidence is produced for extending them. The attempt is to provide limits to arbitrary use by requiring documentation and periodic oversight. However, an analysis seems to find great shortcomings. The wide executive discretion vested under Section 5(2) is heavily reliant on subjective terms like "public emergency" and "public safety", neither of which is defined, leading to the risk of abuse. The absence of mandatory judicial oversight—internal review by the executive, instead—undermines accountability and allows for opaqueness from the affected parties. This arrangement has historically been suitable for telegraphic communication, but it has now proved inadequate in dealing with the complexities of surveillance in the modern age, raising questions over the effectiveness of this Act to protect privacy rights.

Information Technology Act, 2000

The Act presumably extends surveillance into the digital domain and continues to evolve with the advancements in communication technology. By granting power under Section 69 to the government to intercept, monitor, or decrypt any information coming into or out of any computer resource, it expressly states that it is possible for this to be done, such as in the case of sovereignty, national security, public order, or preventing an offense punishable cognizably. This extensive authority becomes applicable to every possible electronic communication such as emails and social media and makes the ambit of the state much larger. This is supplemented by section 69a, allowing blocking of access to online material for those similar reasons, while section 69b allows an authorized body to monitor and collect traffic data for enhancing cybersecurity. The IT (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009 elaborate procedural guidelines requiring written orders from competent authorities and a review every 60 days by a designated committee. However, with these considerations, the fact remains that scope within the IT Act is much wider than scope within the Telegraph Act, which covers only interception, as well as proactive monitoring and collection of data. Quite clearly, a juncture in analysis shows a major flaw- vague terms like "public order" and "national security" are interesting to note, as little or no clarity comes about such terms, and such terms could easily create avenues for abuse, wanting misusing them for other political or non-security reasons. There is no pre-approval from the judiciary in this case, and everything depends on the discretion of the executive, which is once again an echo of the failings of the Telegraph Act but with the volumes of data involved and stakes of privacy higher; it would amplify the problem much more. Critics claim that this framework prioritizes state power over the rights of individuals and lacks the required proportionality established by *K.S. Puttaswamy v. Union of India*[6].

Other Relevant Provisions

Apart from the core legislation, the Digital Personal Data Protection Act, 2023 (DPDP Act) comes with a newly fashioned data governance framework crossing over into surveillance. Section 4 speaks for principles of lawful processing of data, among which is purpose limitation and fairness and Section 7, which permits processing without the consent of the public for purposes of state functions such as security. This exclusion, on the surface, legalizes surveillance activities under the guise of achieving public interest, yet, it turns out, on further analysis, to be very specific as the regulation of direct surveillance is concerned. The DPDP Act is about private data handlers and only addresses state surveillance in some limited way, while Section 7 has such a broad exception that it could even allow the complete unchecked collection of data by government agencies. This is indicative of a piecemeal system whereby privacy rights are lagging behind their power and resulting in no effective deterrent to state encroachment. The law is just beginning to be implemented and will require hitherto judicial interpretation to smooth the creases of any conflict with the older laws like that of IT Act under which it operates with respect to constitutional rights.

---

[4] Sangeeta Mahapatra, "Digital Surveillance and the Threat to Civil Liberties in India", 3 *GIGA Focus Asia* 77 (2021).

[5] (1996) 9 SCC 367.

[6] (2017) 10 SCC 1.

Constitutional Basis

The Indian Constitution is the pedestal on which one can stand and launch a challenge against intrusion into their lives. Article 21 guarantees 'life and personal liberty', which has, in *K.S. Puttaswamy v. Union of India*[7], been read to include privacy as an inherent component of the provision. Such an open understanding of the judicial meaning requires that all such intrusion into individual freedoms, surveillance included, needs to be justified by law, necessity, and proportionality. Article 19(1)(a), though not directly mentioning it, is equally in the purview of this aspect because the effect of such surveillance on communication is a chilling effect on free communication. In short, these constitutional provisions counter the statutory surveillance powers. However, such protection will be useful only as long as there is judicial scrutiny so that the existing laws like the Telegraph and IT Acts are left unscathed and will not deter the executive from exercising that power. Such a situation creates an underlying discontent; while Constitution stands firm on such rampant naked provisions, statutes work on diluting its efficacy with the lane of discretion and lower accountability, thus necessitating the reform procedures for constitutional alignment in state surveillance.[8]

PRIVACY RIGHTS IN INDIA: CONSTITUTIONAL AND JUDICIAL DEVELOPMENTS

In India, the recognition of privacy as a fundamental right is an evolving dynamic shaped through interpretations of the Constitution and landmark judicial decisions that set the environment for surveillance in India. This section shall discuss the constitutional foundation and major judicial developments underlying privacy rights, with a special emphasis on their effect on state monitoring practices.

Constitutional Foundations

Judicial interpretations suggest that, while privacy is undoubtedly implicated in the workings of the Indian Constitution, it does not clearly guarantee this right against arbitrary state action, including surveillance. Article 14 guarantees equality before the law and equal protection, providing a check against any surveillance practice being discriminatory or unjustified. Any action by the state, such as subjecting an individual or group to monitoring without having a reasonable basis for so doing, would, as inferred from this provision, attract an arbitrary tag and be struck down as unconstitutional. In other words, proportionate surveillance of political dissidents or of minority communities that would not in and of itself constitute clear evidence of a threat may violate this equality principle, thereby releasing judicial scrutiny into the actions of the state. Article 19, on the other hand, relates to freedoms of speech, expression, assembly, and association, encroaching upon the matter of privacy. Surveillance, especially of private communication or public gathering, may act as a disincentive to exercise these rights. Knowing that they are being watched, people may self-censor or abstain from public gatherings. The right to Article 19 cannot, however, be subjected to unreasonable restraint, restriction, or regulation, and has constantly been said by the Supreme Court of India to be beyond the broad surveillance powers envisaged by the state. Article 21 establishes the foundation of the whole right of privacy, which deals with the right to life and personal liberty. This interpretation was narrow in the beginning, having grown over decades to include dignity and autonomy, and finally entailing the acceptance of privacy as an integral part. These three articles—14, 19, and 21—set forth a constitutional framework that implicitly seeks to ensure due justification, non-discrimination, and proportionality, and in the event of a breach, this blends into assurance for judicial intervention against the overreach of state powers.[9]

K.S. Puttaswamy v. Union of India

K.S. Puttaswamy v. Union of India[10] is a landmark judgment in Indian constitutional law that recognizes privacy as a fundamental right. The case originated as a challenge to the Aadhaar scheme by the government that did not consider privacy as an independent right under the Constitution. A nine-judge bench unanimously overruled earlier precedents, *M.P. Sharma v. Satish Chandra*[11], which denied constitutional status to privacy. The Court propounded that privacy was intrinsic to Article 21 involving personal autonomy, bodily integrity, and informational self-determination. The rationale was that privacy encases the inner sanctum of an individual's life protecting him from unwarranted state intrusion-including surveillance. A significant principle emerged stipulating that any restriction on privacy such as interception under Section 5(2) of the Indian Telegraph Act, 1885 or Section 69 of the Information Technology Act, 2000 should meet a three-fold test- legality (backed by law), necessity (serving a legitimate aim), and proportionality (least intrusive means). The Court underscored therefore that privacy is not absolute but it has to be delicately balanced with state interests such as security but that balance has to be shown to be demonstrably fair and transparent. The import of Puttaswamy cuts deep and lays down the gold standard for surveillance laws. Thus it necessitates revisiting statutes and practices absent any sufficiently clear safeguard or judicial oversight-such as those with the kind of broad executive discretion currently present in existing frameworks. The judgment has since affected the cases relating to digital privacy and state monitoring, pressuring the government into legitimizing its action against this constitutional standard, thus heightening the legal stature of privacy in India.[12]

---

[7] (2017) 10 SCC 1.

[8] Arjun Harkauli, "The Fine Balance — Surveillance, Security, and the Right to Privacy", *available at:* https://www.scconline.com/blog/post/2023/08/03/the-fine-balance-surveillance-security-and-the-right-to-privacy (last visited on March 4, 2025).

[9] Sidharth, "Surveillance vs. Privacy: Balancing National Security and Individual Rights in India", 12 *International Journal of Creative Research Thoughts* 108 (2024).

[10] (2017) 10 SCC 1.

[11] (1954) SCR 1077.

[12] State Surveillance in India and the Threat to Privacy, *available at:* https://blog.ipleaders.in/state-surveillance-india-threat-privacy (last visited on March 21, 2025).

Post-Puttaswamy Implications

The stage of consideration in surveillance is now tougher due to the constitutional sanctity which privacy has obtained after the Puttaswamy judgment (*K.S. Puttaswamy v. Union of India*[13]); hence, there is greater demand for the alignment of state actions with the legality, necessity and proportionality tests, thereby questioning the arbitrariness of powers provided under statutes such as the IT Act. The Supreme Court in the Pegasus spyware case dated October 27, 2021, referred to Puttaswamy as it questioned the use of sophisticated surveillance tools against journalists and activists by the government and mandated an independent investigation into alleged violations of privacy. This shows the readiness of the judiciary to hold the state accountable, where surveillance should not constitute a means of political oppression. The same sentiments were echoed by the Delhi High Court in *Edward Gomes v. Union of India*[14] regarding the privacy of encrypted WhatsApp messages, maintaining that technological advancements do not diminish constitutional protections. This heightened emphasis on proportionality in the post-Puttaswamy period has rekindled legislative discussion on the Digital Personal Data Protection Act, 2023, but is still limited in preventing state surveillance. The mutual reinforcement of proportionality by the courts has demonstrated that these laws are deficient; neither Rule 419A of the Telegraph Act nor IL Rules 2009 require prior judicial approval and remain opposed to the requirements laid down in Puttaswamy. Such a change has provided more firepower to challenging instances of abuse in surveillance, including cases on social media surveillance and data retention in pursuit of transparency and accountability. Still, the mechanisms for promoting accountability have been inconsistent, with resistance by the executive and legislative inertia stymying much-needed reforms, thereby also leaving privacy rights in a state of flux in their tensions with security needs.

Judicial Interpretations: Key Case Laws

They're judicial interpretations that are instrumental in framing the debate on surveillance and privacy in India-rights of individuals against state security. This part will delve into landmark cases pertaining to such tensions while illustrating the contributions they have made in the standards of law as well as the challenges yet not met.

People's Union for Civil Liberties v. Union of India

Judiciary engagement with surveillance came in from the front with the case of *Peoples*' *Union for Civil Liberties v. Union of India*[15]; dealing with the non-documented practice of telephone tapping in India under the Indian Telegraph Act, 1885. The facts stemmed from a public-interest litigation, challenging unlimited interception of communication without procedural safeguards, on the count of privacy violations. The applicant contended that misuse of Clause 5(2) under that Act, which permits interception on 'public emergencies' or 'for public safety', was being misused by the absence of a clear demarcation infringing the citizens' rights. The Supreme Court recognized a possible abuse by ruling out these kinds of surveillance as an invasion of privacy at a very high level, with a supervision so strict. It instituted significant safeguards: the interception orders have to be by an officer not below the rank of Home Secretary, include with target and the time period, and reviewed by an eminent committee within some time frame. The decision decreed that orders be restricted to a two-month minimum, able to be extended only to six months with adequate justification, and that meticulous documentation of orders be kept for accountability. The significance of this ruling lies in the early problem of privacy-surveillance balance; it happened before privacy was expressly recognized as a fundamental right. The stimulus for this ruling was the absence of statutory procedures, compelling judicial imposition of Rule 419A under the Telegraph Rules-that framework continues to exist today. It also left gaps, based on executive as against judicial oversight, as the system itself had no transparency and no redress for those surveilled. Nonetheless, it has set a foundational but imperfect precedent for future cases.

Pegasus Spyware Case (Supreme Court order, October 27, 2021)

Above all, this is now an issue in a very modern confrontation with the nature of threats against privacy that could be mounted through surveillance technology. The facts arise out of the allegations that the Pegasus software-as-built by the Israeli NSO Group-founded was used in the Indian government interventions against more than 300 individuals, including journalists, activists, and opposition figures. Global investigations, including Amnesty International's, revealed forensic evidence from a cellphone hacker on these targets, bringing the storm of consternation for the state-sponsored assault on how much would be hacked in devices. The petitioners are approaching the courts with the claims of violation of fundamental rights under Articles 19 and 21, as supplemented by *K.S. Puttaswamy v. Union of India*[16]. The process of the Supreme Court took note of the refusal of the government to clarify the nature of its intervention and ruled that allegations such as these should prompt investigation because of their very serious consequences for privacy and freedom of speech. A technical committee was formed, with Justice R.V. Raveendran at its head, to probe the whole affair with emphasis that the cover of national security would not do away with scrutiny of constitutional protections. This case represents the distilling of all the dangers from the new form of technologies for advanced surveillance that went beyond anything else. Pegasus allows unrestricted access to capturing one's private messages, phone calls, and even feeding the camera and alleged penetrating such users'data into the system without any evidence of consent or knowledge of the users themselves. This presents invasion through a dimension that does not yet exist in India's legal framework, particularly in Section 69 of the IT Act, which does not provide for carving out provisions for such advanced devices. The independent authority now insists on appointing its own

[13] (2017) 10 SCC 1.
[14] WP(C) No. 12938/2019.
[15] (1996) 9 SCC 367.
[16] (2017) 10 SCC 1.

observer, which manifests a post-Puttaswamy turn towards privacy in India's post-Puttaswamy environment, with what is still an undecided outcome in investigations, leaving the concerns over enforcement and accountability unaddressed.[17]

Edward Gomes v. Union of India

The Delhi High Court case *Edward Gomes v. Union of India*[18] addressed the issue of privacy in relation to encrypted digital communications. The facts revolved around a challenge to state access to WhatsApp messages, which the petitioner claimed had violated the constitutional guarantees. The lawful authority contended that decryption was necessary for the purpose of security inquiries, relying upon Section 69 of the IT Act, 2000. Upholding the right to privacy, the High Court held that encrypted communications are indeed protected under Article 21, as clarified by *K.S. Puttaswamy v. Union of India*[19]. Any interference with the right, it held, must pass the tests of legality, necessity, and proportionality, and it found the state's justification too vague to override the private correspondence "inherent" in any encrypted communication. The ruling asserted that technological advances make end-to-end encryption stronger rather than weaker in terms of privacy expectations, and it requires that the state change its practices accordingly. This is significant because it applies constitutional tenets in the digital space, where state monitoring is rapidly growing. The ruling applies judicial control over the wide-ranging powers established under the IT Act, suggesting that privacy protections would accompany the new means of communication; however, it allows open the question of how courts might reconcile security needs in cases where a stronger evidence of the threat exists.[20]

Other Cases

Several other cases illustrate a changing position of the judiciary in relation to surveillance and privacy. In the Niira Radia Tapes case (2010-11), the interception of conversations of a corporate lobbyist was done under the Telegraph Act for the purpose of tax evasion investigations. Unfortunately, these tapes got leaked to the media and exposed personalities that were not relevant to the investigation, indicating serious procedural flaws in the execution of surveillance and oversight. Although this was not decided as a case, it opened up public and judicial debate for stricter safeguards, which resulted in changes to Rule 419A. Likewise, *K.S. Puttaswamy v. Union of India*[21], dealing with the Aadhaar scheme yet again after 2017, struck down provisions providing for indiscriminate collection of data by both state and private entities. The Court reiterated that privacy limits state power provisionally invalidated wide surveillance claims made under the Aadhaar Act without any limitation on the consent or purpose. These cases all highlight systemic issues such as leaks, overreach, and inadequate statutory controls, thereby reinforcing the role of the judiciary in curtailing surveillance excesses. They complement landmark judgments by describing practical abuses and judicial efforts to bring the practices of the state into line with the rights guaranteed by the Constitution even though gaps in enforcement still exist, demanding further legal and policy reform.

Threats to Individual Freedoms: Evidence of Misuse

Surveillance is aimed at providing security. But in India, it has gone wrong and has threatened personal freedom. This section discusses some of the documented violations, thereby showing how privacy, free speech, and the right to join an association are compromised along with systemic lack of accountability.

Privacy Violations

A century of state surveillance has continuously assaulted the right to privacy. High-profile scandals have shone the light of exposure on its invasive reach. The Pegasus scandal, under the charge of Amnesty International, brought to the fore that around 300 Indian numbers—some of them journalists, activists, and politicians—were on the target list for hacking. This tool is significantly intrusive in that it can extract messages, emails, and activate cameras on devices, with forensic analysis establishing attempted and successful breaches. In its order of October 27, 2021, the Supreme Court recognized these rather serious breaches of privacy as potential violations of Article 21 rights. However, the shadow cast by the government's refusal to acknowledge or deny its involvement caused uneasiness. In a parallel instance of surveillance misuse, the Niira Radia leak illustrates violation with surveillance at a conventional level. The interceptions of Radia's calls, a corporate lobbyist, were legally authorized under the Indian Telegraph Act, 1885, to investigate tax evasion while leaking personal conversations on a massive scale to the media. The information disclosed had no relevance to the investigation of tax evasion, revealing the personal details of innocent individuals that underlined serious procedural flaws and the absence of measures to obviate such massive violations. Both cases manifest how surveillance by newer tools or by older techniques goes beyond its lawful bounds, compromising the personal autonomy and dignity emphasized in *K.S. Puttaswamy v. Union of India*[22].

[17] The Real Struggle for Privacy and National Security in Terms of Liberty and Surveillance, *available at:* https://theamikusqriae.com/the-real-struggle-for-privacy-and-national-security-in-terms-of-liberty-and-surveillance (last visited on March 11, 2025).
[18] WP(C) No. 12938/2019.
[19] (2017) 10 SCC 1.
[20] Gautam Bhatia, "State Surveillance and the Right to Privacy in India: A Constitutional Biography", 26 State Surveillance and the Right to Privacy in India 129.
[21] (2017) 10 SCC 1.
[22] (2017) 10 SCC 1.

Chilling Effect on Free Speech

Humans used to enjoy full freedom of speech, a right enshrined under Article 19(1)(a). Surveillance now has proven to instill fear of retribution. Using Section 69A of the Information Technology Act, 2000, the government arrests individuals based on social media posts that are not favorable with the government using public order as a cause, among others. For example, dissent over 'Twitter' or 'Facebook'results in charges being made under this provision, generally invoked as a source of prevention through incitement but often seen as suffocating legitimate expression. The citizens now hold a chilling effect because it will refrain them and would prevent them from speaking up. Journalists are not spared either because too, they come under scrutiny at that point. The Pegasus case publicized some of the faces in the media, but it went to the lengths to show that these are actually targets of its activity in order to control the reporting of dissent against the state. This surveillance not only would have its ghost on the lack of transparency concerning the purview but also ends in cajoling journalists toward self-censorship which would, in turn, impact the role of a free press in a democracy. Such are the examples of how tools under the guise of security ended up repackaged to suppress dissent; thus, they directly challenge the constitutional balance between the power of the state and rights of individuals.[23]

Impact on Association

There is no denial that the right to association, also under Article 19, will be compromised when groups exercising the right are surveilled. This is once again evidenced by the Pegasus scandal, among others, as activists and members of the political opposition fall within the scope of surveillance under this program. Such targeting reveals the intent to monitor and disrupt collective acts, protests, or political organization, which are part of the democratic participatory process. For example, environmental activists and human rights defenders, who normally have a critical opinion on certain state policies, are often reported to be facing harassment due to the monitoring activity aimed at creating an atmosphere filled with doubt and fear. This is only an invasion of personal privacy; it also encroaches on collective free assembly, because people will rather shy off from joining purposes with the knowledge that they can be seen. A more significant aggravating factor is that such actions are authorized without any judicial scrutiny, as section 69 of the IT act permits, creating a condition in which state surveillance can be practiced on all associations without any requirement of necessity or proportionality, which is one of the principles laid down in *K.S. Puttaswamy v. Union of India*[24].

Lack of Accountability

But the threats have common roots in a blanket absence of accountability, with surveillance pursuing its agenda under absolute opacity and non-visibility to the public. Now, even as section 5 of the Indian Telegraph Act, 1885, and section 69 of the IT Act, 2000, appear to issue a notice from the law, there is no place in which the wire-tappers are made accountable at all for the scale, take-off priorities or outcome of their operations. Rules 419A and IT Rules, 2009, compel internal evaluations; these, however, are ruled by the executive and are not available for public and affected persons' perusal. Now, take such a case as that of Pegasus: - the statement is neither a confirmation nor a denial, leaving citizenry completely in the dark regarding the possibility of monitoring. Similarly, the Niira Radia leaks originated from within related internal imbalance, yet an official report was never made that described the entire breach or made parties accountable. The whole principle of not making public disclosures completely shields the state from scrutiny and now stands in the way of knocking down such surreptitious surveillance-bears. That is, the system lacks checks like judicial pre-approval or annual reports, typical features of regimes working on the lines of USA's FISA, to ensure that surveillance is consonant with constitutional norms, thereby perpetuating possibilities of intrusion into privacy, speaking, and associating.

International Comparison: Lessons for India

Analysis of the planned surveillance schemes would provide the most-needed knowledge to India on different perspectives concerning how to balance security and privacy. This section thus makes a comparison of the United States and the European models intended to draw lessons for dealing with weaknesses in the Indian situation.[25]

United States

The US surveillance regime is put in place through the FISA, particularly Section 702 for non-US persons not in the US, the collection of foreign intelligence from persons outside the United States. In contrast to wide-reaching statutory provisions in India, the FISA imposes the additional requirement of a warrant, which is issued only after a quasi-judicial procedure conducted by the Foreign Intelligence Surveillance Court (FISC), a specialist court. This court would consider applications submitted by agencies such as the NSA, which are required to show that the specific individuals or groups against whom surveillance measures are being employed are possibly involved in threats to national security and hence should be subjected to surveillance. Section 702 calls for an annual certifying process and minimization procedures to limit incidental collection of information in relation to US citizens, together with a reporting mechanism to Congress for transparency. The Indian framework, in contrast, is heavily weighted in favor of executive discretion under the Indian Telegraph Act of 1885 and the Information Technology Act of 2000. Section 5(2) and Section 69 allow for the order to be made by

[23] The Real Struggle for Privacy and National Security in Terms of Liberty and Surveillance, *available at:* https://theamikusqriae.com/the-real-struggle-for-privacy-and-national-security-in-terms-of-liberty-and-surveillance (last visited on March 17, 2025).

[24] (2017) 10 SCC 1.

[25] Arghish Akolkar, "Government Surveillance Against the Right to Privacy in Matters of Cyberspace in India", 5 *Electronic Journal of Social and Strategic Studies* 38 (2024).

officials such as the home secretary or joint secretary without any prior judicial approval, resulting in opaque and unchallengeable surveillance decisions for affected parties. Judicial oversight in the case of the US model is a measure against arbitrary use of such powers, a safeguard absent in India where internal reviews lack independence. Even though there have been accusations that FISA has been extended to excesses—especially in the post-9/11 era—the very fact that there exists a courtroom with checks from the legislature affords it a clearly defined contrast to India's executive-heavy regime and is testament to which it might find reform.

European Union

The European Union seeks to protect privacy via the General Data Protection Regulation (GDPR), with Article 5 stating that the processing of personal data must comply with the principles of data minimization and transparency. This means that any personal data collected must be adequate, relevant, and limited to the purpose for which it was taken, which is why the principles are directly enforceable by independent national data protection authorities. The regulation applies to private entities and indirectly to state actions and sets high standards of consent and accountability. In Schrems II (C-311/18), the Court of Justice of the European Union tightened the noose on privacy safeguards by invalidating the EU-US Privacy Shield for lacking protection against mass surveillance practices in the US. The ruling asserted that state surveillance should be based on the necessity and proportionality doctrine, where the onus lies on the state to affirmatively demonstrate that there is robust access oversight and controls to avoid indiscriminate data access. The member nations have also integrated judicial review in the interception process under the Regulation of Investigatory Powers Act, 2000, which starkly contrasts with India. For instance, in India, the IT Rules, 2009, allow for such monitoring with limited and sometimes nonexistent public disclosure, whereas the proposed Digital Personal Data Protection Act, 2023, grants Section 7 exemptions for state security while denying independent scrutiny. The lesson for India from the EU is clear: independent oversight-whether via courts or regulators-regulations, and transparent data practices can curb surveillance excess.

Implications for India

The international models make it clear that India needs a rights-oriented surveillance framework, given that its current laws seem to favor security over personal protections. The FISA in the United States has shown that judicial oversight can act as a counterbalance to executive power, ensuring that surveillance is both avowedly targeting and justified-an enormous improvement over the Indian system of an internal committee without judicial involvement. The establishment of a corresponding court or panel would address the unattended discretion wrought by Section 69 orders, thereby fulfilling the proportionality requirement from *K.S. Puttaswamy v. Union of India*[26]. As highlighted by GDPR and Schrems II, data minimization and the existence of independent regulators are principles that are patently absent from Indian statutes that instead permit large-scale data collection without meaningful limits or accountability to the public. Such benchmarks, if implemented, would serve to fine-tune the working of the DPDP Act to limit state exclusions and lay down oversight bodies analogous to the EU data authorities. Characterized by lack of transparency and judicial reviews in its processes, the executive-led system in India stands in stark contrast to the aforementioned regimes, rendering its citizens abjectly vulnerable to magnitude misuse in several well-covered cases. This model, if reformed in the light of development, would have provisions for judicial pre-approval, regular audits, and public reporting, thus bringing a supra-national surveillance regime that would carve out constitutional rights while facilitating security needs, budging closer to the line that demarcates Indian practices from international best practices.[27]

Recommendations for Reform

To amend the already imperfect security frameworks of India's surveillance systems, fine-tuning reforms must balance security imperatives with individual rights in which this section outlines legislative, institutional, transparency, and judicial measures to enhance accountability and safeguard freedoms.

Legislative Reforms

Laws related to surveillance in India are poor and will need a complete overhaul under the legislative changes necessary. The Digital Personal Data Protection Act of 2023 (DPDP Act), while not exhaustive, provides the foundation upon which restrictions against runaway government action must be built. One such area is Section 7, which allows for processing of data without the consent of a person for state security purposes. Such provisions will require serious and time-bound justification instead of blanket concession, aligning this act with privacy principles, limiting its usefulness as a tool for surveillance. Furthermore, an independent law dedicated to the oversight of surveillance is now required and separated from the hodgepodge of the Indian Telegraph Act, 1885, and Information Technology Act, 2000. This legislation might merge intercept powers, define purposes of such events-calling them counter-terrorism or serious crime, and require additional security like purpose limitation and data protection. Borrowed from global models, it must also include penalties for misuse and mechanisms for citizen complaints, focusing on problematic terms like "public order" used in Section 69 of the IT Act. Such reforms provide, in broad strokes, legal groundwork that has a built-in deterrent against arbitrary monitoring while ensuring compliance under Articles 19 and 21 of the Constitution.

[26] (2017) 10 SCC 1.

[27] Bhairav Acharya, "India: Privacy in Peril", *Frontline*, January 1, 1970.

Institutional Safeguards

Proper institutional mechanisms are essential to curb any executive impunity in matters of surveillance. If such a function is to be properly conducted, an independent body, whether it is judicial or parliamentary, would bring in impartial scrutiny, which lacks the current internal review process under Rule 419A and IT Rules, 2009. This body could be made up of judges, legal experts, or elected representatives and would determine whether the requests for surveillance were required and limited to specific threats and not for general populations.

In addition, there should be a requirement that all interception orders be approved by a court of law rather than the executive. A judge, unlike the unilateral decision of the Home Secretary under Section 5(2) of the Telegraph Act, would weigh evidence of risk much like in the US FISA Court. This will ensure that judicial reasoning is incorporated in the system, thus preventing its misuse due to political considerations, and would also work in tandem with the necessity test laid out in *K.S. Puttaswamy v. Union of India*[28], sustaining a system whereby state powers will be exercised responsibly.

Transparency Measures

Transparency is also crucial in restoring trust in government and curbing abuses of surveillance. Another requirement would be public annual reports on surveillance activities, such as: number of orders issued--which agencies are involved and what were the general purposes—but excluding sensitive operational details. Such a practice is normal among jurisdictions like the EU, which provides oversight, but not at the expense of security in contrast to the present current secrecy in India. Clear data retention and destruction policy among other issues are needed. Currently, the IT Act and Telegraph Act do not have such provisions, such as stating how long the intercepted data can be held and when it must be destroyed; therefore, there is a possibility that it could remain indefinitely in storage and be misused. Legislation should prescribe retention periods (for example six months unless extended by a court order) and secure destruction thereafter to ensure that data is not used outside its intended purpose. These measures would create accountability so that citizens could measure the scale at which the state monitors them and also challenge irregularities.

Judicial Enforcement

The judiciary should be active in preserving privacy against surveillance. The proportionality standard in *K.S. Puttaswamy v. Union of India*[29] should be applied with consistency requiring restrictions to be lawful, necessary, and least intrusive in every circumstance. Therefore, surveillance orders would require post facto scrutiny by the courts, and any falling short of this standard would be declared invalid, as was seen in the Pegasus case wherein the Supreme Court passed an order on October 27, 2021, requiring an investigation to be held warranting the breach of user privacy through an absence of weighing of interests. Guidelines issued by the courts could help codify how laws such as Section 69A of the IT Act should comply with this test and hence reduce ambiguity in enforceability. The strength of judicial enforcement guarantees that legislative and institutional reforms are firm in practice, holding the state accountable and asserting privacy over security in the constitutional framework.

Conclusion

As far as concern for the surveillance framework of India is there, it is primarily based on statutes such as Section 5(2) of the Indian Telegraph Act, 1885, and Section 69 of the Information Technology Act, 2000. Such provisions should give the state an omnipotent approach to security. It permits interception as well as monitoring for public safety and national integrity purposes thereby establishing the government's legitimate interest. However, such clauses are wordy and lack strict safeguards like judicial oversight or clear purpose limitations making them prone to overreach. The judiciary has intervened to correct that. In *People*'s *Union for Civil Liberties v. Union of India*[30], for example, the Apex Court introduced procedural checks regarding phone tapping recognizing privacy's importance, while in Pegasus case, the Apex Court warned about use of advanced spyware against own citizens, thereby demanding an investigation. Even after all these initiatives, gaps remain. The lack of mandatory judicial approval and public reporting mechanisms creates a situation wherein surveillance is almost completely unchecked, as evident from reported misuses affecting privacy, speech, and association. Comparison with international systems such as the US and EU further exposes Indian deficiencies with regard to oversight and data protection and underlines the need for a more balanced approach.

The unchecked nature of surveillance in India poses a clear threat to individual freedoms, undermining the constitutional protections of privacy and expression affirmed in *K.S. Puttaswamy v. Union of India*[31]. Under current conditions, security is a primordial function of the State, whereas the complete agency of the executive using such a thin framework as available to supervenes into proper accountability frameworks. Indeed, there is an acute need for reform. Without reform, surveillance will continue to impinge on rights as evidenced in some notorious violations, necessitating a speedy effort to return the system to constitutional principles.

One should develop a legally regulated framework that equally protects privacy and state security. For one, such changes involve updating the Digital Personal Data Protection Act, 2023, to minimize states' exemptions so that surveillance requests may be assessed by properly constituted judicial oversight bodies. Increased transparency from public disclosures and strict controls on the handling of their data by states would enhance accountability. The proportionality principle must be enforced systematically within the judiciary, drawing upon its precedents to offset state excesses. In addition, we should

[28] (2017) 10 SCC 1.
[29] (2017) 10 SCC 1.
[30] (1996) 9 SCC 367.
[31] (2017) 10 SCC 1.

conduct research into other current or emerging technologies, especially where AI gets involved in surveillance, since these systems are now so powerful that they will allow massive states to intrude into the freedoms that systems seek to protect on a continually changing digital platform.