INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 6 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

CONSTITUTIONAL PROTECTION OF THE RIGHT TO PRIVACY: A COMPARATIVE STUDY OF INDIA'S SURVEILLANCE FRAMEWORK WITH REFERENCE TO THE UNITED KINGDOM AND THE UNITED STATES

AUTHOR – ISHRAT AYESHA ATIYA, LLM (CONSTITUTIONAL LAW), AMITY INSTITUTE OF ADVANCED LEGAL STUDIES, AMITY UNIVERSITY UTTAR PRADESH, NOIDA

BEST CITATION – ISHRAT AYESHA ATIYA, CONSTITUTIONAL PROTECTION OF THE RIGHT TO PRIVACY: A COMPARATIVE STUDY OF INDIA'S SURVEILLANCE FRAMEWORK WITH REFERENCE TO THE UNITED KINGDOM AND THE UNITED STATES, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 6 (6) OF 2026, PG. 01-14, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT

The judgement passed by the nine-judge bench in the most famous case of Justice K.S. Puttaswamy v. Union of India (2017) ruled that the right to privacy was now a fundamental right which is protected by Articles 14, 19, and 21 of the Indian Constitution. However, while this was a constitutional breakthrough, India's current surveillance system uses the Indian Telegraph Act (1885) and Information Technology (2000), as the basis of extensive and mostly unregulated surveillance of citizens, allows extensive executive/administrative powers to surveil and do not have prior judicial reviews; do not have independent reviewing bodies; and do not offer individuals meaningful legal recourse. To examine the legality and morality of the surveillance arrangement within Indian Jurisprudence through a doctrinal and comparative analysis of global human rights law and the experiences of the U.K. and U.S. Accordingly, the nature of surveillance and power to "surveil" are structurally unsatisfactory, do not meet the proportionality test per the Puttaswamy Judgement, or India's legal obligations as a signer of the International Covenant on Civil Rights. Targeted reform recommendations at the conclusion of the article include establishing a specific law to regulate surveillance; requiring courts to approve surveillance prior to the arrest and detention of individuals; creating an independent body with authority over surveillance practices; restricting the use of exemptions under the Digital Personal Data Protection Act (2023); and creating mechanisms for the Parliament to oversee intelligence agencies.

Keywords: *Right to Privacy; Article 21; State Surveillance; Proportionality; Comparative Constitutional Law; India; United Kingdom; United States; Digital Personal Data Protection Act, 2023; Puttaswamy.*

INTRODUCTION

The question of privacy is one of the most debated constitutional and human rights issues of our time. With rapid technological change, the growth of digital governance, and the increasing use of data in running government, the relationship between state surveillance and individual liberties has been dramatically changed. In the past, technology and institutional factors limited the ways societies could be surveilled. Today, however, the development of complex and nearly continuous surveillance systems can track our communications, movements, and associations throughout digital ecosystems.

In India, the trajectory of the constitutional right to privacy has changed dramatically, from an early judicial disinclination to a strong judicial acknowledgement of the right. The Supreme Court's nine-judge bench sitting as a

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 6 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Constitution bench (Justice K.S. Puttaswamy v. Union of India, 2017)[1] unanimously determined that the right to privacy is a fundamental right under Articles 14, 19, and 21 of the Constitution[2]. Moreover, the judgement lays out a four-part proportionality framework to evaluate state infringements on privacy: legality goal, necessity, and procedural safeguards.

The Indian government protects citizen's rights to privacy but has limited measures to guarantee their privacy. The current system that regulates surveillance in India is based upon the Indian Telegraph Act of 1885 and the Information Technology Act 2000, two laws that were created long before technology existed. As a result, they do not implement the proportionality principle established in Puttaswamy. However, the Digital Personal Data Protection Act of 2023[3] is a major step towards controlling many of the exceptions that allow for governmental data usage; nonetheless, it diminishes citizen's constitutional protection of privacy.

This article reviews the constitutionality of the current surveillance framework in Inda with formal comparison to that of the United Kingdom and United States. The article is divided into six sections: the constitutional expansion of the right to privacy; the statutory surveillance framework in India; a comparison of the United Kingdom and United States frameworks for surveillance; an overview of significant Supreme Court decisions regarding privacy; the identification of structural issues with India's privacy framework; and recommended reforms to improve privacy in India.

CONSTITUTIONAL EVOLUTION OF THE RIGHT TO PRIVACY IN INDIA

A. Early Judicial Resistance

Privacy was not included in our Constitution during India's formation. Courts ruled against constitutional privacy rights, such as in M.P. Sharma v. Satish Chandra (1954)[4] and Kharak Singh v. State of U.P. (1963)[5]. In M.P. Sharma, the 8- judge bench rules that the Constitutional Framers intentionally excluded provisions similar to the U.S. Constitution's Fourth amendment. The Kharak Singh majority did not find privacy to be an inherent right, but their ruling on midnight incursions at home was a starting point for a group of privacy rights which would require years to develop.

B. Progressive Recognition: Gobind, PUCL, and Rajagopal

In determining whether or not there is a constitutional right to privacy, the Court came to a new conclusion in Gobind v. State of Madhya Pradesh (1975)[6] about the recognition of privacy in terms of personal liberty and privacy, and extended the penumbral rights used in Griswold v. Connecticut (1965) to include privacy as a well as other related areas of law governing these issues. The Supreme Court, in People's Union for Civil Liberties v. Union of India (1997)[7] held that the protections offered by the Telegraph act related to procedural privacy with respect to the telephone were valid, although the executive still had complete control over authorizing telephone tapping by government officials.

C. The Puttaswamy Transformation

In the case of K.S. Puttaswamy v. Union of India, nine judgea unified and reversed both M.P. Sharma and Kharak Singh, reaching a comprehensive constitutional judgement that found privacy to be a basic right inherent in Articles 14, 19, and 21. The Court characterized privacy as a multifaceted right made up of three elements: informational privacy, bodily integrity, and decisional autonomy. The Court decided that no state would be allowed to interfere with the Privacy of an individual unless the state could satisfy four requirements: (i) There is a Valid law, (ii) There is a legitimate

[1] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[2] The Constitution of India, (1950), Arts. 14,19, and 21.
[3] The Digital Personal Data Protection Act, 2023 (Act 22 of 2023)
[4] M.P. Sharma v. Satish Chandra, AIR 1954 SC 300.
[5] Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.
[6] Gobind v. State of Madhya Pradesh, (1975) 2 SCC 148.
[7] People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.

goal for the interference, (iii) Necessary and proportional limitations have to be imposed on the individual's privacy, and (iv) there are sufficient safeguards in place to guarantee that the law does not lead to privacy violations.

The Aadhaar ruling in K.S. Puttaswamy (Retd.) v. Union of India upheld the proportionality principle's application to the State's gathering and use of personal data and declared that all legal provisions permitting unrestricted access to Aadhaar data without any restricts or proportionality were unconstitutional. Most recently, the case of Manohar Lal Sharma v. Union of India[8] has shown the Judiciary's determination to examine Executive claims of surveillance, involving the establishment of an independent Committee to investigate the use of Military Grade Spyware against Members of the Media, Lawyers and Political Leaders.

Following the discussion of the majority holdings discussed in Puttaswamy before Section III. Puttaswamy contributes to our understanding of the law (doctrinal development) in two ways: by providing substantive conclusions about the right to privacy (and other matters) and by providing logic or reasoning for your decision to get there using a variety of analytical lenses (plurality of analytical frameworks). Justice D.Y. Chandrachud's concurrence was a significance contribution to our understanding of the evolution of the information privacy doctrine as a distinct constitutional right. Justice Chandrachud referred to, in particular, a concept from the German

Federal Constitutional Court and used the case judgement from that court in 1983 regarding 'informational self-determination' (otherwise known as the Census Case) to support his conclusion that individuals have a constitutionally protected right to, among other things, how their personal information is collected, stored, processed, or otherwise used. This comparison is also significant in that it supports the notion that information privacy is a foundational liberty that courts should protect to enable individuals to exercise other constitutional rights, including the right to free speech and assembly, and to vote in political elections.

INDIA'S STATUTORY SURVEILLANCE ARCHITECTURE AND ITS CONSTITUTIONAL DEFICITS

A. The Indian Telegraph Act, 1885

Section 5 (2) of the Indian Telegraph Act, 1885 (hereinafter referred to as 'Telegraph Act') gives power to the Centre and the states to intercept communications for purposes including, but not limited to protecting public safety and security, protecting national security, maintaining public order and preventing and investigating crime. Interception is permitted by means of a warrant signed by the Home Secretary, and not by any other legal or judicial process. In its 1997 judgement in PUCL v. Union of India[9], the supreme Court established rules for communication interception, including communications, establishment of a review committee, and maximum permissible time periods for the interception of communications. The review committee created by these guidelines consists entirely of executive level officials and therefore does not provide for any judicial or independent oversight. The issue of having both the authority to approve or deny the request for interception and having the authority to review that request being held by the same structure of government was not addressed through the issuance of the PUCL decision.

B. The Information Technology Act, 2000

Under the Information Technology Act, 2000 (ITA), the government has been given new powers that allow them to capture, watch or open any kind of data held on a computer resource. This gives the government the opportunity to do the same things with all of your online data using the provisions that are used under the Telegraph Act (Section 69).

[8] Manohar Lal Sharma v. Union of India, (2022) 7 SCC 558.

[9] People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.

Section 69A allows blocking of content. Section 69B allows the government the ability to collect traffic data, which is similar to how the United Kingdom collects information from their online users. Neither of these provisions have to have a prior judicial authorization. The IT (Interception, Monitoring and Decryption) Rules of 2009 just follow the executive Review Committee model (of how it would have worked if the Puttaswamy proportionality standard was according to the Constitution). The Supreme Court of India seems likely to rule on the constitutionality of the government's extension of additional powers due to the vagueness, broad nature and the chilling effect due to the effect that it will have free speech because of the Supreme Courts' previous holdings regarding Section 66A in Shreya Singhal v. Union of India (2015)[10]. Tis will likely include all existing grants of power that are vague or too broad in nature under the proportionality test pursuant to Puttaswamy.

C. The Digital Personal Data Protection Act, 2023, and Its Constitutional Limitations

The Digital Personal Data Privacy Act, 2023 is the first comprehensive piece of legislation in India that regulates the protection of personal data. This statute was enacted following the Puttaswamy judgement and lays out the principles and procedures for resolving grievances related to consent, purpose limitation and data minimization. However, Section 17 of the Act[11] permits the Central Government to designate any state instrumentality as being exempted from the provisions of the Act for reasons of national security or public order and does so without first obtaining any judicial approval or independent oversight; this limits how much the Act will cover state-sponsored surveillance of individual's private information. Section 17 fails the necessity and proportionality tests of Puttaswamy's proportionality tests in that it allows blanket executive exemptions without justification being made on a case-by-case basis to replicate the unreviewable executive discretion found with respect to the Telegraph Act's provisions. In short, the Aadhaar decision established that provisions that provide for an absence of necessity and proportionality restrictions for state access to an individual's personal data cannot withstand constitutional scrutiny.

D. The Accountability Gap in Intelligence Agencies

The Intelligence Bureau and Research and Analysis Wing are two of India's main intelligence agencies and do not have any kind of required oversight by Parliament, nor do they have any laws or clear guidelines establishing their powers, duties and limits. These agencies were created through executive orders and therefore conduct their surveillance operations with no oversight from any legislative or independent body. This is arguably a violation of the legality standard set forth by Puttaswamy, which requires that any state action violating an individual's right to privacy must have a law that is (1) clear, (2) available for public review, and (3) sufficiently precise.

E. The Internet Shutdown Regime

One important part of the Court's ruling is that it indicates the proportionality standards that is used in Europe; this standard is set out in the European Convention on Human Rights and is used by the ECtHR as one of four methods to assess whether interference by a state with his privacy rights is valid or not. The ECtHR uses a four-part test for determining if state interference with an individual's right to privacy is appropriate: first, that there is a legitimate aim; second, that the means employed to achieve that aim must bear a reasonable relationship to the objective; third' that the means employed must be necessary and constitute the least restrictive option; and finally, that there are no other reasonable options available. The standard set by the ECtHR for applying this proportionality test (see examples such as S. and Marper v United Kingdom [2008]) has been imported into Indian constitutional law as a strict standard for

[10] Shreya Singhal v. Union of India, (2015) 5 SCC 1.
[11] The Digital Personal Data protection Act, (Act 22 of 2023), s. 17.

judicial review. Earlier cases where the proportionality framework started to develop include Modern Dental College and Research Centre v State of Madhya Pradesh (2016)[12] – prior to Puttaswamy but persuasive authority – where the court also began to apply this proportionality framework as a binding precedent. Consequently, any form of blanket, indiscriminate surveillance and/or aggregate data collection which is not necessary per the proportionality framework is in direct violation of Article 21 of Constitution of India, whether there is express statutory authority.

The Indian government utilizes internet shutdowns as a widespread and poorly studied mechanism to regulate information flow and perform mass surveillance. Most of the internet shutdowns in the country are based on the Temporary Suspension of Telecommunications Services (Public Emergency or Public Safety) Rules, 2017 ("2017 Rules"). These rules were created under Section 7 of the Indian Telegraph Act, 1885.

The Secretary of the State Home Department has the discretionary power to suspend all telecommunications services, including the internet, using the procedures identified in the 2017 Rules (state-level) or the Secretary of the Ministry of Home Affairs (central government) using the procedures identified in the 2017 Rules, if their subjective determination is met by a public emergency and/or danger to public safety. The procedural framework established by the 2017 Rules contains significant flaws which have led to widespread abuse of the Rules.

Although an order must identify (i) the geographic area for which the order applies, (ii) the duration of the order, and (iii) which services to be suspended, orders are not subject to prior judicial review; thus, posing a serious threat to the rule of law and the independence of the judiciary. The Review Committee that is required, by law, to review the orders issued pursuant to the 2017 Rules must complete its review within five (5) days of the order being issued. However, the Review Committee is comprised solely of executive officers; thus, creating major concerns regarding the independence of the Review Committee and the manner in which the Review Committee members will examine and consider the orders. The fact that people cannot find out if they have been suspended because the Indian government does not make suspension orders public makes it difficult for them to challenge suspension orders and defend against them.

The number of internet shutdowns in India (which has continuously been the highest in the World), as documented by the Software Freedom Law Centre which recorded over 700 occurrences from 2012-2020 is profound in its impact on the privacy of individuals. An internet shutdown does not simply limit people's access to information; it removes people's ability to privately communicate; access financial services; seek medical care; or perform any journalistic functions. An internet shutdown functions as a digital form of collective communicative surveillance, with the State having entirely different forms of control over digital communication throughout an entire jurisdiction. The 2017 Rules are also reflective of a structural gap in the privacy framework as they give executive action the ability to violate the information privacy of entire populations without meaningful judicial review in direct opposition to the requirement set by Puttaswami of proportionality.

COMPARATIVE FRAMEWORK: UNITED KINGDOM AND UNITED STATES

A. The United Kingdom: From Executive Practice to Legislative Regulation

For almost 30 years, the ECtHR's decisions regarding the need for a legal basis for surveillance have had a significant impact on creating a framework for surveillance in the U.K. according to the ECtHR, surveillance must be undertaken in accordance with the law (which must be clear, publicly available, predictable

[12] Modern Dental College and Research Centre v. State of Madhya Pradesh, (2016) 7 SCC 353.

and precise to avoid arbitrary application of the law) as established in the Malone v. U.K. (1984)[13] case. The ECtHR found that, sue to the lack of statutory authority allowing for the interception of private communications (in this instance, telephone calls), this was contrary to Article 8 of the ECtHR.

Subsequent to Malone, Parliament enacted legislation which refined the legal framework for surveillance—the Interception of Communications Act 1985, the Regulation of Investigatory Powers Act 2000, and the Investigatory Powers Act 2016[14]. The Investigatory Powers Act (IPA) introduced a 'double approval' authorization system requiring a Secretary of State, along with a Judicial Commissioner, to grant authority to undertake surveillance. The Investigatory Powers Commissioner (IPC) conducts proactive audits and issues annual reports providing information regarding the volume of surveillance carried out, as well as refers cases to the courts for a determination as to whether conduct entitles the individual to compensation. Individuals who believe they are victims of improper surveillance can bring their complaints against the government for resolution before the Investigatory Powers Tribunal.

The Grand Chamber of the European Court of the Human Rights looked at the U.K.'s bulk interception framework in Big Brother Watch and Others v. United Kingdom (2021)[15]. The Grand Chamber held that while bulk interception is not necessarily incompatible with the Human Rights Convention, to meet Convention requirements, there must also exist sufficient end-to-end safeguards, meaning that legislation cannot ensure compliance with human rights through complexity alone.

B. The United States: Constitutional Doctrine and Institutional Oversight

The foundation for U.S. law regarding surveillance is based upon the Fourth Amendment (4A) prohibiting search and seizure without justification (Olmstead v. United States, 1928)[16]. This legal foundation evolved with the introduction of "reasonable expectation of privacy" (Katz v. U.S., 1967)[17]. Prior to Katz, a search was justified when a law dictates that the property owner had exclusive control over it. Thus, "reasonable expectation of privacy" revoked property or trespass laws as a basis for justifying the legality of a lawful search/seizure. The case of United States v. United States District Court (Keith Case) (1972)[18] established that even national security surveillance conducted within the domestic sphere must be pre-approved by a judge and that there is no inherent duty of the executive branch to conduct surveillance without a warrant.

As explained in Carpenter v. United States (2018)[19], there is reasonable expectation of privacy for historical cell site location data (CSLI) under 4A and therefore is entitled to greater constitutional protections than provided for under the third-party doctrine. The reasons for this include: the number of digital records, types of personal data contained within records created, and how that record could be complied into a record of your activities.

In addition to judicial cases, the Foreign Intelligence Surveillance Act of 1978 established a separate tribunal called the Foreign Intelligence Surveillance Court ("FISC") to decide whether national security surveillance orders should be approved or denied. However, the USA PATRIOT Act (2001) extended the government's ability to surveil individuals without traditional warrants/ FISC approvals after September 11; this was somewhat curtailed by the USA FREEDOM Act ("FREEDOM") (2015), which limited the majority collection and use of

[13] Malone v. united Kingdom, (1984) & EHRR 14.
[14] Investigatory Powers Act, 2016 (UK).
[15] Big Brother Watch and Others v. United Kingdom, Application No. 58170/13, 62322/14 and 24960/15 (Grand Chamber, ECtHR, 2021).
[16] Olmstead v. United States, 277 U.S. 438 (1928).
[17] Katz v. united States, 389 U.S. 347 (1967).
[18] United States v. United States District Court, 407 U.S. 297 (1972).
[19] Carpenter v. United States, 585 U.S. 296 (2018).

certain types of data while also creating additional transparency regarding reporting requirements related thereto. Courts have also subsequently recognized that digital information has a different constitutional status than other types of information, such as in the case of Riley v. California (2014)[20], which affirmed that searches of the content on the cell phone incident to a warrantless arrest require a warrant prior to searching that cell phone.

C. Comparative Structural Analysis

A comparative analysis indicates structural differences across all levels. On the legal framework dimension, the United Kingdom's IPA is a comprehensive and specifically written piece of legislation; the United States has the Fourth Amendment combined with the FISA; and India is reliant on pre-colonial laws and generic legislation without any specific law that covers surveillance. In regard to judicial authorization, both the United Kingdom's double-lock system and the United States FISC provide independent judicial review at the time of authorization, whereas Indian law has no requirement for any judicial review.

In terms of independent oversight, both the United Kingdom IPCO and the United States Privacy and Civil Liberties Oversight Board function as an institutionally based oversight entity, whereas India has no equivalent oversight entity. With respect to transparency and redress, both the United Kingdom and United States require periodic reports and institutional procedures for lodging complaints, while no such procedures exist under Indian law.

LANDMARK JUDICIAL DECISIONS

A. Indian Jurisprudence

The Indian courts have evolved for over 70 years, as shown by their interpretations of constitutional issues. Starting with M.P. Sharma (1954) and Kharak Singh (1963), both of which refused to recognize rights created by the constitution, the evolution continued through the decisions in Gobind (1975) and Peoples Union for Civil Liberties (1997) that recognized those rights. In Puttaswamy (2017) the courts affirmed and transformed those rights by recognizing the connection between privacy rights and the Constitution, also upholding that the legislature had failed to create appropriate legislation based on the Constitution.

In the Aadhaar case, the courts ruled that the proportionality framework applied both to digital data infrastructure and to government actions related to digital and biometric information. In Pegasus, the courts established that the Constitution held the executive branch accountable for performing intrusive surveillance when such acts were justified by national security and reiterated that national security justifications could not be used to shield intrusive surveillance from constitutional examination.

In Shreya Singhal (2015), the chilling effect doctrine was recognized as a way in which surveillance suppresses expression and assembly that is constitutionally protected; this overarching lack of transparency regarding India's surveillance regime creates secondary constitutional harms under Articles 19(1)(a) and 19(1)(c). The verdict of the Supreme Court of India, consisting of five judges, in the case of Modern Dental College and Research Centre v. State of Madhya Pradesh (2016) has hastened India's operationalization of proportionality as a constitutional standard. The decision primarily deals with regulating professional education, but its application to proportionality in a constitutional framework is significant for the regulation of surveillance in India.

In its ruling on the regulations governing professional education, the Supreme Court created a four-part structured test requiring that the restriction on the freedom of individuals (e.g. to enter a particular profession) must be:

1. Pursuing a valid purpose.
2. Reasonability linked to achieving that purpose.

[20] Riley v. California, 573 U.S. 373 (2014).

3. The least obstructive means to achieve that purpose.
4. Proportionate, i.e. balancing the infringement of the freedom of an individual's against the importance of the objective to the state.

The proportionality framework subsequently found its way into the analysis of privacy by Justice Puttaswamy, providing a doctrinal foundation for the review of attacks against individuals based on their use of surveillance, ensuring that the state demonstrates that it has adequate justification not only for the existence of surveillance power but also for the extent and intensity of the surveillance.

The proportionality analysis framework for internet governance and the extended internet shutdown enforced in Jammu and Kashmir after having its special constitutional status revoked (August 2019) was applied by the Court in Anuradha Basin v. Union of India (2020), which involved applying the proportionality analysis framework for internet governance. As per Article 19(1) (a) and (g) of the Constitution, both the freedom of speech and expression and the right to engage in digital commerce are protected. As a result, limitations on these rights must conform to the authority of Article 19(2) and (6).Most significantly, Court held that internet shut-down orders must be published, periodically reviewed, & cannot last indefinitely; therefore, Court made it clear such orders have to be published, will need periodic reviews, & cannot go on indefinitely.

Privacy implications of Anuradha Bhasin, however, are significant even if they were not fully contemplated in the judgment itself; Court implicitly acknowledged that state-imposed communicative deprivation by virtue of a failure to provide access to Internet, as well as by way of establishment of Internet shut-downs, affect right to informational privacy in addition to expressive rights. Court's requirement that orders be published and reviewed aligns with "necessity" & "proportionality" elements of Puttaswamy framework. Limitation of judgment is that it did not specifically deal with structural deficits of 2017 Rules, i.e., that judicial preauthorization is not required and Review Committee is comprised solely of executive members, were not challenged. Scholarship subsequent to Anuradha Bhasin has posited that a more complete implementation of proportionality doctrine from Puttaswamy would necessitate that structural reform as a constitutional minimum, and this is not addressed by Digital Personal Data

Protection Act, 2023 because powers associated with internet shutdowns are outside its statutory scope. The Supreme Court of the United States recognized the chilling effect in Laird v. Tatum (1972), and the European Court of Human Rights held in Szabo and Vissy v. Hungary (2016) that simply having laws allowing surveillance will create a chilling effect, with similar principles applying in India.

B. United Kingdom Jurisprudence

The UK courts have shown how critical it is for legislation to be clearly written. Malone (1984) established that you can only limit a person's rights if the law allows you to do so. Halford v. United Kingdom (1997)[21] clarified that this requirement applies to private communication made through the workplace. Khan v. United Kingdom (2001)[22] determined that both statutory and no statutory guidelines must meet the Convention's quality of law standard before they can be considered acceptable. Liberty and Others v. United Kingdom (2009)[23] established that bulk interception regimes must have appropriate oversight mechanisms in place and limit the scope of their use to meet the Convention's requirements. Big Brother Watch (2021) confirmed that even if there is a comprehensive set of legislation regarding bulk interception, sufficient oversight and control must still be documented at the time of legislative enactment—that is a necessary lesson for India's fragmented set of laws on the subject.

[21] Halford v. United Kingdom, (1997) 24 EHRR 523.
[22] Khan v. United Kingdom, (2001) 31 EHRR 45.
[23] Liberty and Others v. United Kingdom, (2009) 48 EHRR 1.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 6 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

C. United States Jurisprudence

U.S. Federal Courts have defined the constitutional evolution necessary for addressing digital surveillance through American case law. The ruling in Katz v. U.S. (1967) shifted the focus of constitutional protections from property-based to person-based. In U.S. v. Keith (1972), the Court established that domestic security surveillance is prohibited without previous consent from the judiciary. The ruling in Clapper v. Amnesty International USA (2013)[24] highlighted the structural justice concerns of covert surveillance because an individual's inability to challenge covert surveillance stems from the inability to prove standing, a similar problem exists in India's opaque interception process. The Court's ruling in Carpenter v. U.S. (2018), demonstrated a measured change in judicial decision-making, by highlighting that the comprehensive, detailed, and retrospective nature of digital data requires a constitutional level of protection that is not currently met by pre-digital doctrine.

D. International Judicial Standards

At the international level, international tribunals have also been influential. The European Court of Human Rights (ECtHR) has advanced a comprehensive jurisprudential framework concerning surveillance over time—from Klass v. Germany (1978), Zakharov v. Russia (2015)[25] and Big Brother Watch v. UK (2021)—that requires a clear legal basis, categorical necessity, independent oversight, limitation of duration, regulation of data storage, and effective individual recourse. Likewise, General Comment No. 16 of the UN Human Rights Committee articulates that the same four fundamental principles of legality, necessity, proportionality, and effective remedy, called for by the ICCPR[26], are mandatorily imposed as a constitutional requirement according to the Supreme Court of India's Puttaswamy ruling.

STRUCTURAL CHALLENGES IN INDIA'S SURVEILLANCE FRAMEWORK

The absence of an explicit and comprehensive legislation regarding surveillance establishes and supports the structural deficiencies within India's constitutional framework on surveillance. The lack of a specific statute in place creates a fragmented legal base for state-sponsored surveillance, which falls under various pre-colonial statutes (such as the Indian Penal Code) (the IPC) and many different general purpose legislative acts (such as The Criminal Procedure Code), whereby executive agencies are able to choose which specific statute to adopt in support of their use of state surveillance.

The executive branch's concentration of authorization and oversight powers (concerning surveillance) will be seen as un-constitutional due to it violating the principle of independent oversight that Puttaswamy and the Keith case both reaffirm. The lack of an independent standing oversight body creates no institutional mechanism for determining the proportionality of interception power applications, the publication of transparency reports or the auditing of the operations of various agencies involved in surveillance.

According to the "legality" competent as laid out in Puttaswamy, along with the case law set forth by the European Court of Human Rights beginning with Malone, terms such as public emergency, public safety, national security and public order are extremely broad and vague in their definitions: thus, are not clear or specific enough to provide sufficient guidance to ensure that the application of these legal concepts is constrained against arbitrary exercise of power.

The lack of any process for notifying individuals and providing them with remedies means that those being subjected to surveillance are generally unaware that they have been surveilled. Thus, the remedies available under Articles 32 and 226 of the Constitution are almost impossible for individuals to access, thus representing a structural justice issue similar to

[24] Clapper v. Amnesty International USA, 568 U.S. 398 (2013).
[25] Zakharov v. Russia, Application No. 47143/06 (ECtHR Grand Chamber, 2015).
[26] International Covenant on Civil and Political Rights, 1966, art. 17.

that in Clapper. The DPDPA's Section 17 replicates bureaucratic discretion as a matter of Executive Authority and effectively violates the constitutional guarantee of implementing privacy as mandated under Puttaswamy.

The rapid introduction of new surveillance technologies, such as facial recognition and AI enhanced CCTV, and large-scale biometric databases, location tracking, at a time when there is no regulatory regime, no data protection standards and no independent oversight, provide the basis for constitutional violations resulting from algorithmic discrimination and mass profiling of a large number of individuals, and do not enjoy any of the constitutional protections that having a warrant has provided as established in Riley v. California and Carpenter.

The challenge presented by algorithmic surveillance is made evident if we look to major state-built infrastructure systems, such as the National Intelligence Grid (NATGRID) and Crime and Criminal Tracking Network and Systems (CCTNS) as examples. NATGRID, which was implemented after the 2008 Mumbai attacks, is being implemented gradually over time through additional operational dates. NATGRID integrates 21 different ministries' and agencies' data, including but not limited to, immigration records, banking transactions, income tax filings, railway and airline reservations, telephone records and more into one network. There are 11 Central security and intelligence agencies that have access to NATGRID information. The significant problem with NATGRID is that it has no statutory basis for its operation; it operates through executive order without Parliamentary authorization, there is no independent oversight mechanism, there is no purpose limitation clause, and there is no requirement for minimum data use. None of these criteria of the Puttaswamy framework that establish an intrusion into privacy must be by law (as described above as "a law" which is, accessible, and foreseeable, and is proportionate relative to the effect on a person's privacy). In the case of NATGRID these requirements for statutory authority have not been me therefore the requirements of Puttaswamy have not been satisfied.

CCTNS is an information-sharing system for police agencies. The National Crime Records Bureau, under the Ministry of Home Affairs, provides the interlinking of police stations across India through one database, which contains first information reports (FIRs), arrest records, and the entire spectrum of a citizen's criminal history at the state level. While it serves a valid law enforcement function, CCTNS also raises concerns that the algorithmic profiling and crime mapping tools layered onto this database can produce predictive risk scores for citizens based upon their residential location, caste, and prior knowledge of police, which are all factors that correlate with systemic discrimination rather than specifically determining a person's propensity for criminal behaviour. Additionally, the absence of a legislative audit mechanism, a right of correction for inaccurate records, or any outside oversight entity converts CCTNS from an ordinary administrative database into a "supervisory" surveillance tool with probable constitutional defects. By specifically exempting the processing of data from the provisions of the Digital Personal Data Privacy Act 2023 for purposes related to "the prevention, detection, investigation and prosecution of crimes," CCTNS denies individuals who are incorrectly classified within these systems of any statutory remedies against the wrongful actions taken by these systems. This creates a vacuum for governance and regulatory controls where litigation based on violations of the Constitution is unlikely to provide an effective solution.

RECOMMENDATIONS FOR REFORM

A. Enacting a Dedicated Surveillance Law

India needs a completely new, independent surveillance law. It should replace not just the existing Telecommunication and Information Technology acts but become the only legal obligation for the State to be able to listen or intercept communications without a warrant. In

doing this, it must clearly define all the types of surveillance that may be carried out, include clear criteria for obtaining authorization to do so, set out how long each recording or interception may be held for, and eliminate evidence after an authorization period of time has expired. The law must also provide procedural safeguards to satisfy the four-part Puttaswamy Test and Article 17 of the International Covenant on Civil and Political Rights.

B. Before Access is Granted to Surveillance Equipment a Third Party must Authorize it

All warrants to permit the interception of communications should be granted by an independent third party, such as the UK's Judicial Commissioner or a member of the US Foreign Intelligence Surveillance Court with sufficient due process and transparency. Although it would be permissible for emergency situations, any emergency surveillance warrants should still be subject to prompt authorization by an independent third party. The Keith decision and Malone decision confirm that authorizing the interception of communication requires independent judicial oversight and is therefore a requirement of the Constitution rather than simply good practice.

C. An independent Surveillance Oversight Commissioner (analogously the IPCO in the United Kingdom)

The statutory powers should oversee the legality and proportionality of agency interception orders through proactive audits, and publish annual reports regarding transparency, and refer matters for judicial or legislative consideration. There are adequate means of ensuring operational confidentiality (for operational safety) without sacrificing accountability of the institutions themselves.

D. The exemptions to the DPDP Act (s 17)

It should be considerably narrowed to require state agencies to seek pre-judicial approval and conduct individualized necessity and proportionality assessments before using their powers to intercept communications. Following the Indian ruling concerning Aadhaar, the unconstitutional invalidation of those provisions authorizing unlimited state interception of communications now has clear constitutional authority.

E. A statutory requirement should be implemented to provide for the notification of individuals

They should be given notification subject to surveillance once the operational safety of such notification no longer exists, together with a system for resolving complaints regarding unlawful surveillance through a standing adjudicatory tribunal. The UK's Investigatory Powers Tribunal could serve as an excellent model. Otherwise, the structural secrecy of India's surveillance regime continues to maintain a justice deficit identified in Clapper and creates practically illusory constitutional rights of redress.

F. Statutory Framework for the Intelligence Agencies

To have the IB and RAW created a statutory framework to establish their powers, functions, and limitations with corresponding parliament oversight pursuant to the creation of a dedicated Intelligence and Security Committee with appropriate clearance/security levels and mandatory access to agency reports. The statutory framework is a constitutional requirement of Parliament accountability under Articles 75 and 105. The lack of a statutory configuration for India's principal agencies is a critical constitutional deficiency.

G. Regulations Governing New Surveillance Technologies

Laws must be established for the use of facial recognition, AI-based surveillance methods, and large-scale biometric systems that require a legal framework with independent oversight, performance assessment, and data minimization. Both Riley v. California and Carpenter demonstrate that the unique qualities of digital information provide for

specific constitutional protections, rather than applying the pre-digital standard mechanically.

CONCLUSION

As articulated in Puttaswamy, privacy is a fundamental constitutional right, which enables people to freely exercise all respect for themselves (e.g., their rights of free speech, right to meet and join groups, and participate in political decision-making). This article documents how India's current framework for conducting physical and technological surveillance of individuals will not reasonably ensure that individuals can exercise their right to privacy consistent with India's constitutional provisions.

The framework used by the Government of India to conduct physical and technologically based surveillance of individuals is essentially based upon the Colonial Era Telegraphed Laws and on existing general IT laws. It concentrates the power to authorize and oversee the surveillance on the executive branch and does not provide for prior judicial approval of any surveillance; nor does it provide for a separate agency to review the reasonableness and legality of the Government's surveillance activities or require the Government to report to the public on its surveillance activities. Rather, the DPDP Act, 2023 does regulate how private sector data will be collected and used but does replicate the same pattern of executive discretion with respect to how state agencies/who will be exempt from the overall requirement and subsequent restrictions; i.e., state actors will routinely be exempt from compliance with the restriction regarding the collection, use and transmission of natural person and/or "personal" data. The accountability gap associated with IB and RAW complicates the lack of oversight and monitoring of the Government's exercise of its significant intelligence authority with no constitutional or statutory or parliamentary accountability.

India's democracy must decide whether to support or not the regulation of governmental surveillance through an independent judicial body. The comparative analyses of the UK and US demonstrate how different countries have achieved this goal using different methodologies of guaranteeing constitutional rights and oversight mechanisms for the regulation of surveillance.

Reforming the aforementioned features of surveillance in India into a single piece of legislative action is necessary to bring India's surveillance law framework into compliance with the ruling in Puttaswamy. The disparity between what was promised under the Puttaswamy decision, and the current status of India's surveillance framework cannot be closed through an incremental process of executive action; rather, it can only be filled through the passing of an integrative, comprehensive legislative reforms that are consistent with the constitutional bases under which Puttaswamy was decided.

The reform agenda described in this paper directly answers each of the three research questions posed at the beginning of the analysis. The first question — whether or not the constitutional acknowledgement of data privacy as an inherent right in Puttaswamy has been turned into practical legislative protections — must be answered negatively. Despite the Digital Personal Data Protection Act 2023 being a legislative improvement, it still does not effectively implement the proportionality outline established by Puttaswamy in various key ways: its government exemption clauses are too large, the consent mechanisms are structurally compromised by notice-and-consent's informational asymmetries, and the Data Protection Board lacks institutional independence necessary to perform oversight of the executive branch. Therefore, the constitutional guarantee set forth in Puttaswamy is still significantly unfulfilled at the statutory level.

The second research question — whether lessons can be drawn from the comparative frameworks of the GDPR and other jurisdictions

— yields a measured affirmation. Although direct adoption cannot be made because India has a vastly different administrative system, federal system, and judicial culture than other countries, many comparable issues do exist. The principles in the GDPR, such as limiting data, restrict developing reasons to collect data, and the idea that citizens have rights to redressal for violations of their privacy (Right to Privacy) are similar in structure to the Proportionality Doctrine as articulated in the Puttaswamy Case. While the GDPR provides statutory authority for the limitation of data per purpose, the TRRB Oversight Body may provide the necessary structural support to develop a privacy-focused framework in India.

The answers to the first two questions (structural and functional limitations of India's data governance framework) lead directly to the third question (What specific reforms are needed to remedy the identified structural deficits?). The necessary reforms are; (1) Statutory Authority for NATGRID and CCTNS with limitations on their purposes, (2) Judicial Authorization (by the higher judiciary) for Blocking Internet Access, (3) An Independent Data Protection Authority with enforcement authority, (4) Appellate Authority for All Data Protection Matters, (5) Algorithmic Impact Assessments Must Be Conducted Prior to Data Sharing, (6) A Non-Derogable Requirement for Limited Data Collection in National Security Matters, (7) Dramatic Changes to the Existing Data Subject Rights Framework to Allow for Effective Enforcement Against Government Entities; and (8) In-Built Protection of the Right to Privacy (Including Encryption). Collectively, these structural reforms will operationalize the Puttaswamy Decision, protecting all persons' right to privacy as recognized by international law and affirming the need for such protection in practice, not just on paper.

References

A. Constitutional Provisions and Statutes

1. Constitution of India, 1950: Articles 14, 19, 21, 32, 226.
2. Indian Telegraph Act, 1885 (Act No. 13 of 1885)
3. Information Technology Act, 2000 (Act No. 21 of 2000)
4. Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009
5. Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023)
6. Investigatory Powers Act, 2016 (UK)
7. Foreign Intelligence Surveillance Act, 50 U.S.C., Sec. 1801-1885 (USA)
8. International Covenant on Civil and Political Rights, 1966: Article 17
9. Universal Declaration of Human Rights, 1948: Article 12.

B. Cases

1. K.S. Puttaswamy vs. Union of India, (2017) 10 SCC 1 (Supreme Court)
2. K.S. Puttaswamy (Retd.) vs. Union of India (Aadhaar), (2018) 1 SCC 809 (Supreme Court)
3. Manohar Lal Sharma vs. Union of India, (2022) 7 SCC 558 (Supreme Court)
4. People's Union for Civil Liberties vs. Union of India, (1997) 1 SCC 301 (Supreme Court)
5. Gobind vs. State of Madhya Pradesh, (1975) 2 SCC 148 (Supreme Court)
6. R. Rajagopal vs. State of Tamil Nadu, (1994) 6 SCC 632 (Supreme Court)
7. Kharak Singh vs. State of Uttar Pradesh, AIR 1963 SC 1295 (Supreme Court)
8. M.P. Sharma vs. Satish Chandra, AIR 1954 SC 300 (Supreme Court).
9. Shreya Singhal vs. Union of India, (2015) 5 SCC 1 (Supreme Court).
10. Modern Dental College and Research Centre vs. State of Madhya Pradesh, (2016) 7 SCC 353 (Supreme Court).
11. Big Brother Watch and Others v. United Kingdom, Application No. 58170/13, 62322/14 and 24960/15 (Grand Chamber, European Court of Human Rights, 2021).
12. Malone v. United Kingdom, (1984) 7 EHRR 14.

13. Halford v. United Kingdom, (1997) 24 EHRR 523.
14. Khan v. United Kingdom, (2001) 31 EHRR 45.
15. Zakharov v. Russia, Application No. 47143/06 (European Court of Human Rights, Grand Chamber, 2015).
16. Carpenter v. United States, 585 U.S. 296 (2018).
17. Katz v. United States, 389 U.S. 347 (1967).
18. Riley v. California, 573 U.S. 373 (2014).
19. United States v. United States District Court (Keith Case), 407 U.S. 297 (1972).
20. Clapper v. Amnesty International USA, 568 U.S. 398 (2013).
21. Olmstead v. United States, 277 U.S. 438 (1928).