The Infinite
An International Peer Reviewed / Refereed Journal of Multidisciplinary Research

An Online Peer Reviewed / Refereed Journal
Special Issue (Volume 2| Issue 1) | October 2025
ISSN: 3048-9539 (Online)
Website: www.theinfinite.co.in

Surveillance, Privacy, and National Security: The Constitutional Dilemma

Dr. Santosh Kumar

B.Sc. (Maths), LL.M., NET, JRF, SRF, Ph.D. (LAW)

ARTICLE DETAILS

Research Paper

Keywords :

Surveillance, Privacy, National Security, Constitution, Human Rights, Comparative Law.

ABSTRACT

The tension between state surveillance and the individual's right to privacy represents one of the most profound constitutional dilemmas of the twenty-first century. Governments worldwide justify intrusive surveillance measures as necessary tools to protect national security, combat terrorism, and ensure public safety. Yet these same measures risk undermining the fundamental liberties and dignity that constitutional democracies are built upon. This paper critically examines the relationship between surveillance, privacy, and national security through a comparative constitutional lens, focusing primarily on India while drawing parallels from the United States and the United Kingdom.

The study begins by exploring the conceptual foundations of privacy and surveillance, tracing their evolution in constitutional jurisprudence. It analyzes India's privacy framework under Article 21 of the Constitution, particularly after the landmark judgment in K.S. Puttaswamy v. Union of India (2017), and examines the legislative instruments—such as the Information Technology Act, 2000, and the Indian Telegraph Act, 1885—that empower state surveillance. Comparatively, it considers U.S. approaches under the Fourth Amendment and U.K. mechanisms under the Investigatory Powers Act, 2016, and European Convention jurisprudence.

The paper argues that while national security imperatives are legitimate, they cannot override constitutional guarantees without due

process, necessity, and proportionality. It advocates for transparent oversight mechanisms, judicial authorization of surveillance, data protection legislation, and international human rights standards as prerequisites for ethical and lawful state surveillance. The study concludes that a democratic state's legitimacy depends not on the breadth of its surveillance powers but on the constitutional constraints governing their use.

1. Introduction

In the digital age, where every click, call, and conversation leaves a trace, the boundaries between privacy and state surveillance have become increasingly porous. Surveillance technologies—ranging from CCTV networks and mobile interception to facial recognition and artificial intelligence—grant states unprecedented power to monitor citizens. Proponents of such measures argue that enhanced surveillance is indispensable to counter terrorism, prevent cybercrime, and safeguard national integrity. Yet, this same technological omnipresence poses existential threats to civil liberties and the democratic ethos.

The constitutional challenge lies in striking a delicate balance between two competing imperatives: the state's duty to ensure national security and the individual's right to privacy and freedom. Both values are essential to democracy; yet, excessive emphasis on one can easily erode the other. When unchecked, surveillance transforms from a security instrument into a mechanism of control, chilling dissent, eroding trust, and infringing autonomy.

India, the world's largest democracy, exemplifies this dilemma. With a population exceeding 1.4 billion and rapidly expanding digital infrastructure, surveillance practices have intensified in scope and sophistication. The legal regime—anchored in colonial-era statutes like the Telegraph Act, 1885, and supplemented by the Information Technology Act, 2000—grants broad interception powers to the executive with minimal independent oversight. Judicial recognition of privacy as a fundamental right in *K.S. Puttaswamy v. Union of India* (2017) has, however, introduced new constitutional constraints, demanding that state surveillance satisfy tests of legality, necessity, and proportionality.

At the global level, debates surrounding mass surveillance gained prominence following Edward Snowden's 2013 revelations about the U.S. National Security Agency's (NSA) programs, which exposed pervasive collection of communication data worldwide. Similarly, the U.K.'s Investigatory Powers Act, 2016—dubbed the "Snooper's Charter"—illustrates the expanding reach of surveillance powers in liberal

democracies. Despite variations in legal frameworks, all three jurisdictions wrestle with the same fundamental tension: how to reconcile national security imperatives with the constitutional promise of individual liberty.

This paper aims to analyze this constitutional dilemma by integrating doctrinal, comparative, and normative perspectives. It explores how different constitutional systems conceptualize privacy, the extent to which surveillance powers are legally constrained, and the ethical limits of state monitoring. The analysis reveals that although each jurisdiction attempts to balance privacy and security differently, all face similar challenges of overreach, opacity, and inadequate accountability.

2. Conceptual Framework: Privacy, Surveillance, and National Security

2.1 The Meaning of Privacy

Privacy, as a legal concept, defies simple definition. It encompasses autonomy over personal choices, control over information, and protection from unwarranted intrusion. The U.S. Supreme Court in *Griswold v. Connecticut* (1965) defined privacy as the right to be "let alone," shielding individuals from state interference in intimate decisions. In India, *Justice K.S. Puttaswamy v. Union of India* (2017) expanded this understanding, recognizing privacy as intrinsic to human dignity and liberty under Article 21 of the Constitution.

Scholars have identified multiple dimensions of privacy:

- Informational privacy, which protects control over personal data.
- Decisional privacy, encompassing reproductive and bodily autonomy.
- Spatial privacy, safeguarding the sanctity of home and communication.

In modern constitutionalism, privacy operates as both a negative right (protecting individuals from state intrusion) and a positive right (imposing duties on the state to secure privacy through law and regulation).

2.2 Surveillance and Its Constitutional Implications

Surveillance refers to the systematic observation, recording, or analysis of individuals' activities, communications, or data. Historically, surveillance was physical and limited; today, it is algorithmic, pervasive, and often invisible. State surveillance can be classified into:

- Targeted surveillance, justified for specific threats and subject to judicial approval.
- Mass surveillance, indiscriminate collection of data affecting entire populations.

While targeted surveillance may be constitutionally defensible under due process, mass surveillance poses profound constitutional and ethical risks. It undermines freedom of expression (Article 19(1)(a)), association (Article 19(1)(c)), and due process (Article 21), creating what scholars term a "chilling effect" on democratic participation.

2.3 The National Security Justification

National security is a legitimate state objective; no constitutional order can survive without safeguarding its integrity. Yet, as Justice D.Y. Chandrachud cautioned in *Puttaswamy*, "the mere invocation of national security cannot override the fundamental right to privacy." Surveillance undertaken in the name of security must meet strict constitutional tests of legality (statutory basis), necessity (least restrictive means), and proportionality (balancing public interest and individual rights).

The "national security exception" has often been invoked expansively by states to justify intrusive surveillance. The lack of independent oversight mechanisms, secrecy of intelligence operations, and technological complexity make it difficult to ensure accountability. The constitutional dilemma thus lies in preventing legitimate security objectives from morphing into tools of authoritarian control.

2.4 The Democratic Paradox

Democracy requires both security and freedom. Surveillance ostensibly protects democracy by preventing threats, yet it simultaneously undermines democracy when used to suppress dissent or monitor citizens. This paradox underscores the constitutional tension central to this paper: *Can a state safeguard its people without spying on them?*

3. The Indian Constitutional Context

3.1 Evolution of Privacy in Indian Jurisprudence

The Indian Constitution does not explicitly mention the right to privacy. However, judicial interpretation has progressively read it into the broader guarantee of life and personal liberty under Article 21. The trajectory began modestly in *Kharak Singh v. State of Uttar Pradesh* (1963), where the Supreme Court invalidated police "domiciliary visits" at night but refused to recognize privacy as a distinct fundamental right. Justice Subba Rao's dissent, however, foreshadowed modern privacy jurisprudence by declaring that "the right to personal liberty takes within its sweep the right to be free from encroachments on one's privacy."

The Court revisited this in *Gobind v. State of Madhya Pradesh* (1975), recognizing privacy as a fundamental right subject to reasonable restrictions. Later decisions, including *R. Rajagopal v. State of Tamil Nadu* (1994), affirmed privacy as a facet of freedom of expression and autonomy. This doctrinal evolution culminated in the landmark nine-judge bench decision of *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), where the Supreme Court unanimously declared privacy a fundamental right under Articles 14, 19, and 21.

3.2 The *Puttaswamy* Framework: Legality, Necessity, and Proportionality

In *Puttaswamy*, the Court articulated a threefold test for any state action infringing privacy:

1. **Legality** – There must be a law that authorizes the encroachment.
2. **Legitimate Aim** – The law must pursue a legitimate state interest such as national security, public order, or prevention of crime.
3. **Proportionality** – The extent of interference must be necessary and proportionate to the aim pursued.

This test provides the constitutional yardstick for evaluating surveillance laws and practices. It ensures that the state cannot rely on broad, discretionary powers without statutory authorization or judicial scrutiny.

3.3 Legislative Framework Governing Surveillance

India's surveillance architecture operates through multiple statutes, many of which predate the digital era. These include:

3.3.1 The Indian Telegraph Act, 1885

Section 5(2) of the Telegraph Act, 1885 authorizes interception of messages "on the occurrence of any public emergency" or "in the interest of public safety," provided it is necessary in the interest of national security, public order, or preventing incitement to an offense. This provision, a colonial relic, remains the legal basis for telephone tapping. In *People's Union for Civil Liberties (PUCL) v. Union of India* (1997), the Supreme Court held that phone tapping violates privacy unless conducted under lawful authorization. The Court laid down procedural safeguards such as recording reasons, time limits, and review committees. However, the Act's vague terms ("public emergency," "public safety") and executive discretion continue to invite criticism.

3.3.2 The Information Technology Act, 2000

Section 69 of the Information Technology Act, 2000 empowers the central and state governments to "intercept, monitor, or decrypt" electronic information in the interest of sovereignty, defense, or public order. The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 prescribe procedures, including approval by a competent authority and periodic review. Critics argue these rules confer excessive executive power with limited judicial oversight, contrary to the *Puttaswamy* standards.

Additionally, Section 69A authorizes the blocking of public access to online content, while Rule 4(2) of the 2021 IT (Intermediary Guidelines and Digital Media Ethics Code) Rules mandates social media intermediaries to identify the "first originator" of messages—effectively enabling traceability and undermining encryption.

3.3.3 Other Laws and Programs

Other surveillance mechanisms operate through:

- **Central Monitoring System (CMS):** A centralized interception platform allowing direct access to telecom networks by government agencies.
- **NATGRID (National Intelligence Grid):** Integrates databases from various agencies for real-time intelligence sharing.
- **Aadhaar Project:** Although intended for welfare delivery, it has raised privacy concerns over biometric data collection.
- **CCTV Surveillance Schemes:** State governments have increasingly mandated installation of public surveillance cameras without explicit data protection safeguards.

Together, these programs form a complex surveillance ecosystem with minimal parliamentary oversight or transparency.

3.4 Judicial Approach Post-*Puttaswamy*

3.4.1 PUCL v. Union of India (1997)

Before *Puttaswamy, PUCL* established basic procedural safeguards against arbitrary telephone tapping. The Court mandated written authorization by the Home Secretary, periodic reviews, and destruction of

intercepted records after six months. However, the case did not address digital surveillance or mass interception programs.

3.4.2 ***K.S. Puttaswamy v. Union of India*** *(2017)*

The privacy judgment in *Puttaswamy* revolutionized Indian constitutional law. The Court recognized informational privacy as part of personal liberty, emphasizing that state surveillance must adhere to legality, necessity, and proportionality. Importantly, Justice Chandrachud warned against "the creation of a surveillance state," stressing that technology must be subordinate to constitutional values.

3.4.3 ***Puttaswamy (Aadhaar)*** *(2018)*

In the subsequent Aadhaar case, a five-judge bench upheld the Aadhaar scheme for welfare purposes but struck down provisions allowing private companies access to biometric data. The judgment reaffirmed privacy safeguards while accepting limited surveillance justified by legitimate state aims.

3.4.4 ***Pegasus Spyware Controversy (2021–2022)***

In 2021, investigative reports revealed that Pegasus spyware, developed by Israel's NSO Group, was allegedly used to surveil journalists, activists, and opposition figures in India. Petitions before the Supreme Court alleged violation of privacy and abuse of state power. The Court appointed a Technical Committee to investigate, emphasizing that "the state cannot get a free pass by merely invoking national security." The Committee's report (2022) did not publicly confirm state culpability but revealed gaps in surveillance accountability. The case underscored the urgent need for statutory oversight and transparency.

3.5 Data Protection and Oversight Mechanisms

India lacks a comprehensive data protection regime comparable to the EU's GDPR. The Digital Personal Data Protection Act, 2023, recently enacted, introduces consent-based processing but includes broad exemptions for government surveillance "in the interest of sovereignty and security." These exemptions risk undermining privacy protections unless narrowly interpreted and accompanied by independent review.

Current oversight mechanisms are largely executive in nature. The Review Committee, constituted under surveillance rules, comprises only senior bureaucrats. There is no judicial warrant requirement, no independent regulator, and no obligation to notify affected individuals. As scholars note, "India's surveillance regime operates in a legal vacuum of accountability."

3.6 Constitutional Tension: Liberty versus Security

Indian constitutionalism seeks to harmonize individual liberty with collective security. Article 21 guarantees the right to life and personal liberty, while Article 19 ensures freedoms of expression, association, and movement—all vulnerable to surveillance overreach. The state's duty to protect sovereignty and integrity is equally rooted in the Directive Principles and Preamble.

However, the Constitution does not prescribe absolute hierarchies among rights. The *Puttaswamy* test of proportionality requires that infringements be necessary, least intrusive, and justified by compelling state interest. Yet, in practice, Indian surveillance operates through opaque executive orders, often without legislative or judicial authorization. This imbalance—between constitutional ideals and administrative reality—constitutes the core of India's privacy-security dilemma.

3.7 The Emerging Debate on Democratic Oversight

Civil society and scholars have increasingly called for a Parliamentary Committee on Surveillance Oversight and a Judicial Authorization Regime akin to U.S. and U.K. models. Proposals include:

- Requiring judicial warrants for surveillance, especially digital interception.
- Periodic public reporting of aggregated surveillance statistics.
- Establishing a Data Protection Authority with investigatory powers.
- Incorporating privacy impact assessments for new surveillance technologies.

While these proposals remain aspirational, they signal growing recognition that unchecked surveillance endangers constitutional democracy.

3.8 Summary

India's surveillance framework reflects a paradox: a vibrant democracy governed by archaic colonial laws and executive discretion. Judicial developments like *Puttaswamy* have strengthened privacy norms but have yet to translate into robust institutional reform. The legal architecture remains fragmented and opaque, allowing security imperatives to overshadow constitutional accountability.

India's challenge, therefore, lies not in choosing between privacy and security but in reconciling them through constitutional design—ensuring that surveillance remains lawful, proportionate, and subject to democratic oversight.

4. The United States and United Kingdom: Comparative Perspectives

4.1 The United States: Surveillance, Security, and the Fourth Amendment

The U.S. constitutional framework for privacy and surveillance is grounded primarily in the Fourth Amendment, which protects citizens against "unreasonable searches and seizures" and mandates that warrants be issued only upon probable cause. Historically, the Fourth Amendment was intended to prevent physical intrusions by state agents. However, technological advances—from wiretapping to mass digital surveillance—have expanded its scope and complexity.

4.1.1 Early Jurisprudence and the Evolution of Privacy Doctrine

The American understanding of privacy evolved significantly over time. In *Olmstead v. United States* (1928), the Supreme Court held that wiretapping did not violate the Fourth Amendment because it involved no physical trespass. Justice Louis Brandeis's famous dissent, however, envisioned privacy as the "right to be let alone," presaging modern digital rights jurisprudence.

The Court overruled *Olmstead* in *Katz v. United States* (1967), establishing that "the Fourth Amendment protects people, not places." The "reasonable expectation of privacy" test became central: if a person exhibits a subjective expectation of privacy that society recognizes as reasonable, governmental intrusion requires a warrant. This shift from property-based to expectation-based reasoning marked a constitutional expansion of privacy protections.

Subsequent cases—such as *United States v. Jones* (2012) on GPS tracking and *Carpenter v. United States* (2018) on cell-site location data—extended privacy to digital data. In *Carpenter*, the Court ruled that accessing historical cell phone location records without a warrant violates the Fourth Amendment, recognizing the unique sensitivity of digital data and the potential for pervasive surveillance.

4.1.2 Statutory Regime and Post-9/11 Developments

The terrorist attacks of September 11, 2001, fundamentally reshaped the U.S. surveillance landscape. The USA PATRIOT Act (2001) significantly expanded government powers to collect and share information for counterterrorism purposes. Section 215, in particular, allowed the National Security Agency (NSA) to collect bulk telecommunication metadata, including call records of millions of Americans, without individualized warrants.

Following revelations by Edward Snowden in 2013, which exposed programs like PRISM and XKeyscore, public outrage led to partial reforms. The USA FREEDOM Act (2015) curtailed bulk metadata collection, requiring the government to seek records from telecommunication companies under more specific criteria.

The Foreign Intelligence Surveillance Act (FISA, 1978) and its amendments establish a special Foreign Intelligence Surveillance Court (FISC) to issue secret warrants for national security investigations. Critics argue that the FISC operates with minimal transparency and rarely denies government requests, raising questions about meaningful judicial oversight.

4.1.3 The Constitutional Dilemma in the U.S. Context

The U.S. faces a persistent tension between national security exceptionalism and constitutional safeguards. The "state secrets doctrine" often prevents courts from reviewing surveillance programs on national security grounds. Civil libertarians argue this undermines the rule of law. Conversely, proponents contend that secrecy is indispensable for intelligence operations.

The Supreme Court has attempted to reconcile these interests by emphasizing reasonableness over absolute privacy. Yet as *Carpenter* illustrates, digital surveillance's ubiquity has forced the judiciary to reinterpret reasonableness in light of technological realities. The debate continues over whether bulk data collection constitutes an unreasonable search and whether algorithmic profiling requires judicial warrants.

4.2 The United Kingdom: Security, Surveillance, and Human Rights

The United Kingdom presents a contrasting model—a parliamentary democracy without a codified constitution but governed by common law principles, the Human Rights Act 1998, and European Convention on Human Rights (ECHR) obligations.

4.2.1 Evolution of Privacy and Surveillance Law in the UK

Historically, British law lacked explicit privacy rights. The Regulation of Investigatory Powers Act (RIPA) 2000 was the first comprehensive legislation to regulate interception, surveillance, and data access by security and law enforcement agencies. RIPA authorized interception of communications "in the interests of national security" but faced criticism for granting excessive executive discretion and inadequate oversight.

Following sustained criticism and litigation before the European Court of Human Rights (ECtHR), the U.K. replaced RIPA with the Investigatory Powers Act (IPA) 2016, popularly known as the "Snooper's Charter." The IPA consolidated surveillance powers, including interception, equipment interference, and

bulk data collection, while introducing new safeguards such as "double lock authorization" (requiring both ministerial and judicial approval) and oversight by the Investigatory Powers Commissioner.

4.2.2 The Human Rights Framework: Article 8 of the ECHR

The right to privacy in the U.K. is primarily derived from Article 8 of the European Convention on Human Rights, which protects the right to respect for private and family life. Article 8(2) allows interference by public authorities only if it is lawful, necessary, and proportionate in pursuit of legitimate aims, including national security.

In *Liberty and Others v. United Kingdom* (2008), the ECtHR held that the U.K.'s surveillance regime under the Interception of Communications Act 1985 lacked adequate safeguards and violated Article 8. Similarly, in *Big Brother Watch and Others v. United Kingdom* (2021), the Grand Chamber of the ECtHR found that the bulk interception regime under RIPA violated privacy and freedom of expression due to insufficient oversight and safeguards.

These judgments compelled the U.K. to strengthen procedural safeguards in the IPA, emphasizing proportionality, transparency, and necessity—principles aligning closely with India's *Puttaswamy* test.

4.2.3 Institutional Oversight Mechanisms

The U.K. surveillance system operates under a multilayered oversight structure:

- Judicial Commissioners review ministerial warrants to ensure legality and proportionality.
- The Investigatory Powers Commissioner's Office (IPCO) monitors compliance and reports to Parliament.
- Parliament's Intelligence and Security Committee (ISC) provides democratic oversight of intelligence agencies.

These mechanisms collectively reflect a commitment to balancing operational secrecy with constitutional accountability.

4.2.4 Technological Expansion and Current Challenges

The U.K. has increasingly integrated artificial intelligence, facial recognition, and predictive policing into its security apparatus. However, in *Bridges v. South Wales Police* (2020), the Court of Appeal held that live facial recognition technology breached privacy and data protection rights due to lack of legal clarity

and safeguards. The judgment reaffirmed that emerging surveillance technologies must comply with the proportionality principles under the Human Rights Act (1998) and Data Protection Act (2018).

Despite these safeguards, critics argue that the IPA still enables mass surveillance under the pretext of national security, particularly through bulk data collection and data retention mandates. Civil society organizations such as Liberty and Privacy International continue to challenge these provisions before domestic and European courts.

4.3 Comparative Observations: United States vs. United Kingdom

4.3.1 Constitutional Structure

The U.S. model is rooted in constitutional rights and judicial review, while the U.K. relies on statutory and parliamentary oversight under the human rights framework. In the U.S., privacy is constitutionally entrenched in the Fourth Amendment; in the U.K., it arises from international human rights obligations and legislative safeguards.

4.3.2 Judicial vs. Executive Oversight

The U.S. system grants surveillance warrants through the secret Foreign Intelligence Surveillance Court (FISC)—a judicial body, albeit criticized for limited transparency. The U.K. model, in contrast, emphasizes "double lock" authorization, requiring both executive and judicial approval before surveillance commences. The dual authorization mechanism arguably provides stronger preemptive oversight.

4.3.3 Proportionality and Public Accountability

Both systems employ proportionality principles, though the U.K.'s reliance on the ECHR framework embeds proportionality as a central legal requirement. The U.S. courts interpret reasonableness within the context of expectations of privacy—a more flexible but less predictable test.

Public accountability is greater in the U.K. due to annual reports by the IPCO and parliamentary scrutiny, while U.S. surveillance remains heavily shrouded in secrecy under national security exceptions.

4.3.4 Lessons for India

The comparative study offers valuable lessons for India:

1. **Codification and Transparency:** Both the U.S. and U.K. have codified surveillance powers through detailed statutes; India still relies on colonial and executive orders.

2. **Judicial Authorization:** India lacks pre-authorization by independent judges, unlike the U.K.'s double lock or the U.S. FISC model.
3. **Parliamentary Oversight:** India has no standing intelligence oversight committee akin to the U.K.'s ISC.
4. **Periodic Review and Reporting:** Transparency measures such as public reporting on interception statistics could enhance accountability.

India can thus draw from these systems to develop its own rights-based surveillance framework consistent with constitutional values.

4.4 The Shared Democratic Dilemma

Despite institutional differences, the U.S., U.K., and India confront the same fundamental constitutional dilemma: *how to reconcile the imperatives of national security with the sanctity of individual privacy.* Each jurisdiction oscillates between secrecy and accountability, innovation and intrusion, liberty and order.

Technological evolution magnifies this dilemma. Artificial intelligence, big data analytics, and cross-border information flows have rendered traditional legal doctrines inadequate. Whether through the Fourth Amendment's reasonableness test, Article 8's proportionality standard, or Article 21's dignity clause, constitutional systems must evolve to ensure that security measures remain compatible with democratic legitimacy.

As the U.K. and U.S. experiences show, effective oversight, judicial authorization, and transparency can coexist with robust national security. India's future challenge is to institutionalize these safeguards within its own constitutional and administrative architecture.

5. Comparative Constitutional Analysis and Ethical Challenges

5.1 Constitutional Commonalities and Divergences

Across democratic jurisdictions—India, the United States, and the United Kingdom—the constitutional framework governing surveillance and privacy reveals a shared democratic dilemma: the state's duty to protect public safety often collides with the individual's right to privacy and autonomy. Despite different constitutional structures, three common elements emerge: the rule of law, proportionality, and oversight.

5.1.1 Rule of Law and Legality

The principle of legality forms the first line of defense against arbitrary state action. In the U.S., surveillance requires a statutory or judicial authorization under the Foreign Intelligence Surveillance Act (1978). In the U.K., the Investigatory Powers Act (2016) explicitly codifies permissible surveillance activities, creating transparency and procedural safeguards. India, by contrast, relies on Section 5(2) of the Telegraph Act (1885) and Section 69 of the IT Act (2000)—broad provisions that lack detailed legislative safeguards and parliamentary oversight.

While all three jurisdictions recognize legality as foundational, India's surveillance framework remains largely executive-driven, allowing the state considerable discretion. This divergence underscores the need for India to move toward a comprehensive data protection and surveillance regulation with parliamentary accountability and judicial preauthorization.

5.1.2 Proportionality and Necessity

The proportionality test is the key constitutional balancing mechanism. It demands that limitations on privacy must serve a legitimate purpose and be the least intrusive means of achieving that purpose. The European Court of Human Rights (through *Big Brother Watch v. U.K.*, 2021) and the Indian Supreme Court (*Puttaswamy*, 2017) both emphasize proportionality as essential to protecting privacy. In the United States, the standard manifests through the "reasonableness" clause of the Fourth Amendment.

However, proportionality's practical application varies. In the U.S., national security claims often limit judicial scrutiny under the "state secrets doctrine." In contrast, the U.K. and Europe have developed stronger procedural tests, requiring ex ante judicial or independent review. India's challenge lies in operationalizing proportionality—ensuring that security measures are demonstrably necessary and narrowly tailored, rather than pretexts for political or administrative surveillance.

5.1.3 Oversight and Accountability

Oversight is the linchpin of a constitutionally compliant surveillance regime. The U.S. employs judicial authorization through the FISA Court but suffers from opacity. The U.K. supplements executive authorization with Judicial Commissioners and a Parliamentary Intelligence and Security Committee (ISC). India lacks both judicial authorization and parliamentary oversight; its review committees are composed of executive officers reviewing their own actions.

A comparative perspective thus reveals a hierarchy of accountability: U.K. > U.S. > India, in terms of procedural safeguards. The absence of independent oversight in India risks transforming surveillance from a tool of security into an instrument of control.

5.2 Ethical Dilemmas in Surveillance

Constitutional doctrine addresses legality and proportionality, but deeper ethical questions remain unresolved:

- Is there a moral limit to how much surveillance a democracy can conduct on its citizens?
- Can consent or awareness justify data collection for security?
- Does technological capability automatically confer moral legitimacy?

These questions transcend positive law and strike at the philosophical core of democratic governance.

5.2.1 The Utilitarian Justification

Governments often invoke utilitarian ethics—the idea that surveillance serves the greater good by preventing harm to society. National security surveillance is thus justified as maximizing overall welfare, even if individual rights are constrained. However, critics argue that utilitarian reasoning erodes constitutional morality: it treats privacy as a negotiable commodity rather than an intrinsic human value. In a democracy, rights protect minorities and dissenters precisely against majoritarian utilitarianism.

5.2.2 Deontological and Rights-Based Ethics

From a deontological (duty-based) standpoint, individuals possess inviolable rights—privacy, dignity, and autonomy—that cannot be overridden solely for collective utility. Surveillance that violates these intrinsic rights without due process violates the Kantian principle of respect for persons as ends in themselves. The *Puttaswamy* judgment, with its emphasis on dignity, reflects this rights-based ethos.

5.2.3 The "Panopticon" and the Psychological Cost

The concept of the Panopticon, proposed by Jeremy Bentham and later analyzed by Michel Foucault (1977), symbolizes how surveillance creates self-regulating behavior through fear of observation. Even without active monitoring, the perception of being watched curtails freedom of thought and expression. The "chilling effect" undermines democratic participation, academic freedom, and journalistic independence.

In societies like India, where dissent and activism are vital to constitutional democracy, mass surveillance risks producing conformity through invisible coercion.

5.3 Technological Advancements and Constitutional Lag

Surveillance today transcends traditional wiretapping or interception; it is algorithmic, predictive, and pervasive. Governments use big data analytics, facial recognition, drones, and biometric identifiers for "predictive policing" and "smart governance." Yet these technologies outpace legal safeguards, creating what scholars term "constitutional lag."

5.3.1 Artificial Intelligence and Profiling

Algorithmic surveillance involves analyzing vast datasets to detect "anomalous" behavior. However, as studies show (Barocas & Selbst, 2016; Crawford, 2021), algorithmic models often reproduce racial, gender, or socio-economic biases embedded in training data. Predictive policing, for example, disproportionately targets minority communities. Without transparency in algorithms or accountability for outcomes, such systems risk institutionalizing discrimination under a veil of neutrality.

5.3.2 Biometric Surveillance

India's Aadhaar project, the world's largest biometric database, illustrates both the potential and peril of technological governance. Although intended for welfare efficiency, linking Aadhaar to banking, mobile, and welfare databases facilitates profiling and surveillance. In *Puttaswamy (Aadhaar)* (2018), the Court upheld Aadhaar's constitutionality but restricted private use, recognizing the dangers of surveillance capitalism.

In contrast, the U.K. and E.U. have imposed stricter controls on biometric data under the GDPR, classifying it as "sensitive personal data" requiring explicit consent and special safeguards. India's emerging Digital Personal Data Protection Act, 2023, while progressive, allows broad government exemptions for national security—potentially undermining the principle of consent.

5.3.3 Cross-Border Data Sharing and Cloud Surveillance

The rise of global tech giants has blurred jurisdictional boundaries. Data stored on foreign servers is often accessible to intelligence agencies under mutual assistance treaties or secret agreements. The U.S. CLOUD Act (2018) allows American authorities to compel tech companies to produce data stored overseas. Such transnational surveillance raises concerns about digital sovereignty and the extraterritorial application of domestic laws.

India has advocated for data localization to ensure governmental control, yet localization alone cannot guarantee privacy unless accompanied by oversight and rights-based safeguards.

5.4 The Security–Liberty Paradox in Democratic Societies

5.4.1 National Security as an Expanding Exception

The phrase "national security" functions as a constitutional trump card, invoked to justify extensive surveillance powers. Yet, as Justice Chandrachud observed in *Puttaswamy*, "The mere invocation of national security does not render the state immune from judicial scrutiny."

In both India and the U.S., courts have historically deferred to the executive in security matters, especially during crises—the Emergency (1975–77) in India and post-9/11 period in the U.S. However, such deference risks normalizing extraordinary powers. Democracies must ensure that security exceptionalism remains temporary, narrowly tailored, and reviewable.

5.4.2 The Illusion of Safety

Empirical studies suggest that mass surveillance often fails to demonstrably enhance security. The U.S. Privacy and Civil Liberties Oversight Board (2014) concluded that bulk telephony metadata collection under Section 215 of the PATRIOT Act had "minimal unique value" in counterterrorism. Similarly, the U.K.'s Investigatory Powers Tribunal has questioned whether bulk data collection yields proportional security benefits.

This raises the ethical question: *Is it morally justifiable to infringe millions of citizens' privacy for marginal gains in security?* From a constitutional standpoint, proportionality demands measurable effectiveness—security claims must be evidence-based, not speculative.

5.4.3 Surveillance and Chilling Effect on Democracy

The chilling effect—where citizens self-censor for fear of surveillance—poses a grave threat to democracy. It suppresses dissent, inhibits journalistic investigation, and weakens accountability. In India, the use of Pegasus spyware against journalists and activists exemplifies how surveillance can weaponize fear, undermining democratic discourse.

The constitutional cost of surveillance is not only legal but cultural: it alters citizens' perception of state power. When fear replaces trust, democracy's moral foundation erodes.

5.5 Towards Ethical Constitutionalism

To navigate this dilemma, democracies must embed ethics within constitutional governance. Ethical constitutionalism implies that even when law permits surveillance, morality and constitutional conscience should restrain abuse.

This approach demands:

- Transparency and truth-telling about the scope and nature of surveillance programs.
- Public accountability through independent commissions and periodic audits.
- Ethical training for intelligence agencies emphasizing constitutional duties.
- Proportional redress mechanisms for victims of unlawful surveillance.

In short, ethical AI and surveillance governance must be built on the triad of legality, legitimacy, and morality.

6. Recommendations, Policy Reforms, and Conclusion

6.1 Policy and Legal Recommendations

The comparative analysis of India, the United States, and the United Kingdom reveals that constitutional democracies can reconcile national security imperatives with privacy through a combination of transparency, oversight, and proportionality. India, in particular, must transition from executive-centric secrecy to rights-based, institutionally accountable surveillance governance.

6.1.1 Enact a Comprehensive Surveillance Law

India urgently requires a dedicated, post-constitutional surveillance statute—not just fragmented provisions under the Telegraph and IT Acts. This law should clearly define:

1. **Scope and purpose of surveillance**—limiting it strictly to legitimate state interests (terrorism, espionage, national security).
2. **Procedural safeguards**—requiring judicial warrants, time limits, and review mechanisms.
3. **Independent authorization**—separating executive request from judicial approval, similar to the U.K.'s "double lock" system.
4. **Obligation to notify** individuals after surveillance ends (subject to national security exceptions).

5. **Transparency obligations**—mandatory publication of annual interception statistics and audit reports.

Such codification would bring India in line with constitutional democracies where surveillance powers are tightly regulated by statute rather than executive orders.

6.1.2 Judicial Authorization and Review

Independent judicial authorization should be mandatory before interception, decryption, or monitoring. India can adopt a model similar to the Foreign Intelligence Surveillance Court (FISC) in the U.S. or Judicial Commissioners in the U.K.

Judicial review must not be retrospective alone. Ex ante oversight ensures that legality and proportionality are assessed before rights are infringed. The judiciary must also possess the authority to invalidate warrants obtained through false or vague national security claims.

6.1.3 Parliamentary and Independent Oversight

The Indian Parliament should establish a Standing Committee on Intelligence and Surveillance Oversight empowered to:

- Scrutinize surveillance budgets and operations;
- Review policy guidelines; and
- Publish non-sensitive reports for public accountability.

An Independent Surveillance and Data Protection Authority—autonomous from the executive—should monitor compliance, investigate complaints, and issue binding recommendations. This dual mechanism ensures both democratic and technocratic oversight.

6.1.4 Data Protection with Limited Security Exemptions

The Digital Personal Data Protection Act, 2023 should be amended to narrow its broad "national security" exemption. Any derogation from privacy must satisfy the *Puttaswamy* proportionality test. Data retention periods should be minimized, and metadata collection must be subjected to the same standards as content interception.

Adopting data minimization and purpose limitation principles will prevent indiscriminate data hoarding. Further, sensitive data like biometrics or health records should require explicit consent even in security contexts, unless judicially approved.

6.1.5 Algorithmic and AI-Based Surveillance Regulation

Emerging surveillance technologies—facial recognition, predictive policing, AI-based profiling—demand explicit regulation. India should:

- Mandate algorithmic transparency for all AI-based surveillance tools used by the state.
- Require Algorithmic Impact Assessments (AIAs) similar to environmental assessments.
- Enforce independent bias audits to ensure systems do not discriminate on caste, religion, or gender.
- Establish a Code of Ethics for AI in Law Enforcement, aligned with UNESCO and OECD principles.

AI regulation must treat fairness and explainability as constitutional obligations, not optional design choices.

6.1.6 Strengthen Whistleblower and Press Protections

Investigative journalism and whistleblowing are critical to exposing abuses of surveillance power. The Whistle Blowers Protection Act, 2014 should be strengthened to include protections for those revealing illegal surveillance. Additionally, surveillance of journalists should require judicial sanction and be justified by compelling evidence of national threat.

6.1.7 International Cooperation and Human Rights Alignment

India should ratify or align with international privacy standards such as the Council of Europe's Convention 108+ and adopt principles from the UN High Commissioner's Reports on the Right to Privacy in the Digital Age (2018, 2021). Cross-border data requests should follow transparent, rights-respecting frameworks—eschewing secret intelligence-sharing arrangements that evade accountability.

6.2 Comparative Lessons and Theoretical Synthesis

The tension between privacy and surveillance is not unique to India but structural to all liberal democracies. The U.S., U.K., and Indian experiences illustrate differing institutional responses to the same constitutional dilemma.

6.2.1 Institutional Balance

- The U.S. emphasizes judicial authorization (FISC) but struggles with secrecy.
- The U.K. stresses dual authorization and parliamentary oversight.
- India, while rich in constitutional doctrine, remains institutionally weak on enforcement.

Therefore, India's most urgent task is institutional capacity-building—creating structures that give life to constitutional principles.

6.2.2 From National Security to Human Security

Traditional "national security" perspectives equate surveillance with state survival. However, modern constitutional thought advocates a shift toward human security—protecting individuals from violence, discrimination, and loss of dignity. Surveillance that erodes privacy undermines the very security it seeks to preserve. The challenge is not to abolish surveillance but to humanize it through ethics, legality, and accountability.

6.2.3 Technological Neutrality of Constitutional Rights

The *Puttaswamy* judgment established that constitutional rights must evolve with technology. Similarly, in *Carpenter v. United States* (2018), the U.S. Supreme Court recognized that digital data warrants heightened protection. These cases reflect a shared understanding that technology cannot dilute fundamental rights; it must be subjected to them.

Hence, constitutional interpretation must remain technologically neutral yet principally anchored—ensuring that innovation strengthens rather than undermines liberty.

6.2.4 Ethical Governance and Public Trust

The legitimacy of democratic governance depends on public trust. Surveillance conducted in secrecy erodes that trust, leading to democratic alienation. Conversely, when citizens are assured of oversight and remedies, surveillance becomes a legitimate, limited instrument of security rather than a tool of domination.

Thus, ethical constitutionalism—embedding moral responsibility into statecraft—becomes the ultimate safeguard. As Justice Harlan once observed, "The Constitution must be read not as a code of rules but as a living embodiment of moral order."

6.3 Future Pathways: A Rights-Based Surveillance Model

To reconcile privacy with national security, democracies must adopt a Rights-Based Surveillance Model (RBSM) founded on five pillars:

1. **Legality:** Every act of surveillance must have explicit statutory backing subject to judicial review.

2. **Proportionality:** Surveillance must be necessary, narrowly targeted, and the least intrusive means available.
3. **Accountability:** Independent regulators and courts must supervise surveillance and publish periodic reports.
4. **Transparency:** Citizens must have access to aggregate data on state surveillance and avenues for redress.
5. **Remedy:** Victims of unlawful surveillance should have enforceable rights to compensation and correction.

Adopting this model would align India and other democracies with global human rights jurisprudence while preserving legitimate security capabilities.

7. Conclusion

The digital age has redefined both power and privacy. The state now possesses technological tools to monitor its citizens with precision unimaginable to past generations. While surveillance is not inherently unconstitutional, its unchecked expansion imperils the foundations of democracy.This paper has demonstrated that the constitutional dilemma lies not in choosing between privacy and security but in balancing them through proportionality, legality, and accountability. India's post-*Puttaswamy* jurisprudence offers a moral compass, but its statutory architecture lags behind. The United States and the United Kingdom provide instructive contrasts: where judicial oversight, parliamentary scrutiny, and human rights frameworks temper executive power.

Ultimately, constitutional democracy must ensure that the security of the nation does not become the insecurity of its citizens. A state that surveils without restraint ceases to be a guardian of liberty and becomes its adversary. The preservation of privacy is not an obstacle to security; it is its precondition. As Justice Chandrachud wrote in *Puttaswamy* (2017), "The refrain of national security cannot be used to brush aside the right to privacy. The mere invocation of these words does not confer a talismanic immunity from judicial review."The challenge of the twenty-first century, therefore, is not to dismantle surveillance but to constitutionalize it—to embed ethical, legal, and institutional safeguards ensuring that technology serves humanity rather than controls it.Only by aligning surveillance with constitutional morality can a nation secure both its freedom and its future.

References

Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *California Law Review, 104*(3), 671–732. https://doi.org/10.15779/Z38BG31

Basu, D. D. (2022). *Introduction to the Constitution of India* (25th ed.). LexisNexis Butterworths.

Bennett, C. J., & Lyon, D. (2019). *Playing the identity card: Surveillance, security and identification in global perspective.* Routledge.

Carpenter v. United States, 138 S. Ct. 2206 (2018).

Crawford, K. (2021). *Atlas of AI: Power, politics, and the planetary costs of artificial intelligence.* Yale University Press. https://doi.org/10.2307/j.ctv1f70jd9

European Court of Human Rights. (2021). *Big Brother Watch and Others v. the United Kingdom* (Applications nos. 58170/13, 62322/14 and 24960/15). Retrieved from https://hudoc.echr.coe.int

Foucault, M. (1977). *Discipline and punish: The birth of the prison.* Vintage Books.

Katz v. United States, 389 U.S. 347 (1967).

K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India). Retrieved from https://main.sci.gov.in

Latonero, M. (2018). *Governing artificial intelligence: Upholding human rights & dignity.* Data & Society Research Institute. https://datasociety.net

Liberty and Others v. United Kingdom, App. No. 58243/00, 2008 ECHR 568.

Narain, S. (2020). Privacy, national security and the Indian Constitution. *Indian Journal of Constitutional Law, 12*(2), 145–172.

O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy.* Crown Publishing.

People's Union for Civil Liberties v. Union of India, AIR 1997 SC 568 (India).

Regulation of Investigatory Powers Act 2000, U.K.

Supreme Court of India. (2018). *Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar Case).*

The Investigatory Powers Act 2016, U.K.

United States v. Jones, 565 U.S. 400 (2012).

USA PATRIOT Act, Pub. L. No. 107–56, 115 Stat. 272 (2001).

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193–220. https://doi.org/10.2307/1321160