SUPREMO AMICUS

VOLUME 40 | February, 2026 ISSN 2456-9704

PRIVACY RIGHTS AND NATIONAL SECURITY: A LEGAL AND POLICY ANALYSIS IN INDIA

By *Prakhar Vishwakarma*
From *Christ University Pune Lavasa Campus*

By *Amrutha Rose J Valavi*
Assistant Professor at Christ University Pune Lavasa Campus

ABSTRACT

This research paper analyses in critical terms the complicated and dynamic nature of the relationship between the basic right to privacy and the need for national security in India, a tension which has been escalated by the rampant digitalisation, opportunities of broad levels of state surveillance and the development of sophisticated technological resources. Even though the article 21-based constitutionalisation of privacy in Justice K.S. Puttaswamy (2017) and the formulation of legality, necessity, and proportionality constitute the most timely judicial ruling, the statutory and institutional interpretation of surveillance is archaic, disjointed, and relying on the overall use of executive discretion. Older laws like the Indian Telegraph Act, 1885, and the Information Technology Act, 2000 still control modern surveillance methods like AI-based analytics, facial recognition, metadata aggregation, and zero-click spyware like Pegasus despite being poorly suited to the modern threats of smart surveillance systems.

The article combines constitutional law, legislation, and technological changes, and comparisons with how things have worked in the United Kingdom, European Union, and post-Snowden changes in the United States, to point out structural flaws in Indian oversight, transparency and accountability processes. Using case studies on Pegasus, interception and blocking orders, and the National Intelligence Grid (NATGRID), the study shows how regulatory opaqueness has remained a persistent problem, judicial pre-authorisation has not been established, there have been no independent audit reviews, and executive surveillance authority has grown unchecked.

One of the key contributions of the paper is that it reveals significant research gaps: the unavailability of empirical data on the surveillance practice; little research has been done to examine algorithmic policing and AI-based systems; there is no transparency in the acquisition of spyware; insufficient research has been done on the cross-border access to data; and less focus has been made on scrutinizing mandatory digital ecosystems that undermine meaningful consent. These gaps demonstrate the critical necessity of interdisciplinary studies which involve law, technology, public policy and human rights.

The paper has concluded with detailed policy proposals such as a modern Surveillance Reform Act, compulsory judicial or independent approval of high-risk surveillance, provision of enhanced use of oversight commissions, reduced exemptions under the DPDP Act, open procurement of surveillance technologies and use of privacy-protective technical designs.

Finally, the research also states that privacy protection does not undermine national security; instead, a constitutional, transparent, and answerable surveillance system builds people's trust and improves the democratic resilience of India in an ever-data-driven security field.

INTRODUCTION

The accelerated digitalisation of India during the last decade in the form of ever growing smartphone adoption, digitisation of welfare programmes by the state, the growing popularity of online service malls and the growing reliance on data-driven governance has put the rights to privacy and national security in the centre of current legal debates. With India moving into a hyper connected information society, both the State and the non-governmental players assemble, process and store large amounts of personal information.Such a change has brought about complicated weak sections that may be abused by non-state actors, cybercriminals, aggressive foreign organizations, and even the State itself via intrusive surveillance. At the same time, the threats to national security no longer represent a traditional territorial and localized pattern but a high-tech cyber threat, encrypted communication systems, warfare based on artificial intelligence or cross-border digital espionage. Such overlapping imperatives have resulted in what comes to be regarded as one of the most baffling constitutional dilemmas of the current day to what extent should the principle of privacy as fundamental right and the demands of national security as practical and strategic be legally and institutionally resolved in India? The decision of the Supreme Court in the case of K.S. Puttaswamy v. Union of India, privacy has been created as a right under the fundamental right of personal liberty and dignity established under Article 21. Thus, the Court established a constitution by which invasion of privacy by the state should meet the requirement of the test of legality, necessity, and proportionality. The post Puttaswamy judgment environment has however seen simultaneous growth in the capacity of states to spy. The Aadhaar-based authentication ecosystem, the establishment of the National Intelligence Grid (NATGRID), the widespread use of facial recognition technology, extensive interception authority under Section 69 of the Information Technology Act and the Indian Telegraph Act and the claims of the use of Pegasus spyware have all cast very dark doubts on the sufficiency of protection, transparency measures and accountability frameworks. These changes suggest that although the constitution is articulating privacy very strongly, institutional practices and statutory regimes tend to have security imperatives in a manner that can lead to erosion of individual rights, considering these tensions, this research paper will critically examine the legal and policy structure on the issue of privacy and national security in India. It looks at the way constitutional dogma, legislative policies, executive policies and judicial controls interact to influence the equilibrium between personal liberty and national safety. The joint research questions and objectives that will help in this study are: How do the existing laws in India control the intersection of privacy and national security, especially in the areas of surveillance, data processing, and gathering of intelligence? What are the structural weaknesses in regard to oversight, transparency, and accountability? What are some of the new technological and geopolitical realities that make this balance more difficult? More importantly, what can India do to revise its regulation systems so that national security processes are constitutional, fair and in a technologically sound manner? Although the paper is mainly based on the Indian legal system, it uses comparative experience of the Investigatory Powers Act in the United Kingdom, GDPR regime in the European Union, and post Snowden FISA reforms in the United States. These models can teach a great deal about democratic monitoring, external control and regulatory proportionality. This paper will synthesize constitutional doctrine and technology policy, and comparative regulatory practices with the view to making a contribution towards current scholarly and policy discussions regarding the future of privacy and security regulation in India. Finally, the paper attempts to advance suggestions of actionable, constitutionally based and technologically viable reforms to ensure

that the national security system in India is consistent with its national democratic commitment.

LITERATURE REVIEW

The field of academic and policy research on the intersection of privacy and national security in India has grown significantly since the publication of a landmark ruling by the Supreme Court of India under the title Justice K.S. Puttaswamy v. Union of India (2017). This literature represents an active and developing discussion including constitutional theory, technology law, surveillance studies and comparative public law.The works of scholars like Gautam Bhatia, Usha Ramanathan, Ananth Padmanabhan, Vrinda Bhandari and Chinmayi Arun have influenced modern-day knowledge on informational privacy and consequences of state surveillance on the constitution. These authors have a general conceptualisation of privacy as not just a negative right to secrecy but as a multidimensional assurance which comprises decisional autonomy, bodily integrity and the right to informational self determination. Based on the jurisprudence of the world, including the proportionality doctrine of the European Court of Human Rights, the data protection standards of the EU, as well as the Fourth Amendment case law of the US, Indian scholars have pointed that the contemporary issue of privacy is intensely bound to digital systems, algorithmic processing, and the growing presence of state power.

A large part of the literature is questioning the Puttaswamy ruling itself, particularly its application of the three part proportionality test as a constitutional protection against arbitrary state encroachment. Scholars see the verdict as a part of a doctrinal change and a structure that will be used to reform surveillance in the future. A number of the studies highlight Pre-Puttaswamy jurisprudence, especially PUCL v. Union of India (1997) that addressed the issue of telephone tapping- was based on pre-modern technological assumptions and offered little protective measures in procedures. As of 2017, the discussion maintains that the spread of digital surveillance technology, including mass metadata acquisition and high-tech spyware, makes the current case law insufficient. These discussions underscore the fact that the jurisprudence of privacy should keep up with the emerging technological potentials and geopolitical conditions that are evolving at a very fast rate.

Another focus has been on the think tank literature. Organisations like the Internet Freedom Foundation (IFF), Centre for Communication Governance (CCG) at NLU Delhi, Carnegie India, Centre for Internet and Society (CIS), and Observer Research Foundation (ORF) have done critical reports and policy briefs over lapses in the governance of surveillance in India. These evaluations keep identifying structural gaps: the lack of independent oversight mechanisms, the lack of transparency in the authorisation procedures, the lack of the requirement to publish interception statistics on the part of the agencies, and the use of the opaque mechanism in executive decision making. In addition, literature in the field of policy observes that India does not have a single law on surveillance; rather, it is spread over sectoral laws and executive regulations, which offer varying and incoherent protection.

There is a strong vein of criticism of the statutory law of surveillance, especially the Indian Telegraph Act, 1885, and the Information Technology Act, 2000. The Telegraph Act, written in a colonial framework of regulating telegraph lines, allows broad powers of interception in the event of a public emergency, or for reasons of public safety, but without any current definitions or substantive procedural limits. Literature sources emphasize that these outdated standards do not comply with the proportionality requirements that are supported in Puttaswamy. Similarly, the IT act of Section 69 and its subsidiary rules authorise government agencies to intercept, monitor and decrypt computer resources, but scholars claim that such provisions lack judicial checks and balances and they have general grounds of authorisation and they grant wide discretion to the executive.

The introduction of the Digital Personal Data Protection (DPDP) Act, 2023, has created a new

literature review on the impact of the law on privacy and national security. Indeed, commentators admit that the Act provides a legal framework of personal data processing but stress that the Act provides broad exemptions to the State especially when it comes to national security, law enforcement, and public order related activities. Researchers express concerns about the permissibility of these exemptions, lack of independence and power to adjudicate of the Data Protection Board, and the lack of a comprehensive rights-based approach to data principals, and extensive central government rule-making power. Critics claim that the absence of substantive checks and balances will enable the DPDP Act to authorise a wide range of surveillance instead of limiting it.

Comparative international scholarship can bring some good lessons on how democracies strike a balance between surveillance authorities and the rights of individuals. The EU GDPR has high principles of limitation of purpose, minimisation of data, limitation of storage and clear rights of destined data subjects but has highly limited and proportionate security related derogations. The United Kingdom has provided significant protections under the Investigatory Powers Act (IPA) 2016 which establishes the so-called double-lock system of authorizing warrants to conduct surveillance by a Secretary of State, combined with a Judicial Commissioner, compulsory transparency reports, and supervision by independent statutory offices. The post-Snowden literature in the US indicates reforms of the Foreign Intelligence Surveillance Act (FISA), increased judicial supervision, amici curiae adversarial access in some instances, and disclosure requirements.

There is a lot of normative or doctrinal literature and little empirical study has been conducted on how the powers of surveillance are implemented in practice. Publicly available information on the number of interception orders each year, the operation of review committees and on the technological sophistication of intelligence systems like NATGRID, CMS or state police surveillance units is only available sparingly. Scholarship too has lagged behind in adopting new digital technologies like facial recognition, predictive policing algorithms, behavioural analytics and database linking platforms. The socio-legal implications of the surveillance on such vulnerable communities as journalists, activists, minorities, and political dissidents are also under-researched.

On the whole, the literature provides a good conceptual base where one can identify privacy and national security in India but demonstrates little involvement with empirical realities, technological developments, and institutional activities. These loopholes highlight why interdisciplinary literature is necessary based on constitutional law, technology research, government policy, and human rights perspectives, a goal that should be achieved in this paper.

LEGAL AND POLICY FRAMEWORK IN INDIA

The legal and policy framework in privacy and national security in India is at a cross road between the constitutional doctrine, statutory authorisation and a more sophisticated surveillance architecture. Although privacy is an important right in the Indian constitutional order, the statutory environment remains based on the old colonial laws and is coupled with the current digital governance programmes. The result of this duality is a polarizing regulatory environment where power of states has grown very fast without any strong checks and balances. A review of constitutional underpinnings, statutory tools and operational surveillance programmes demonstrate an elaborate structure of high levels of discretion of the state, lack of accountability, and lack of legislative modernisation.

The right to privacy was deeply rooted in the constitutional basis in Justice K.S. Puttaswamy (Retd.). v. Union of India (2017). This was a landmark ruling by the Supreme Court where a 9 judge bench court ruled that privacy is inherent to the provisions of Articles 14, 19, and 21, and thus, it is a fundamental right. The Court expressed a three-pronged doctrine test, including legality, necessity, and proportionality, which should regulate any action of state infringing

privacy. Within this paradigm, State surveillance should not only be legalised by a legitimate law, but it should also have a legitimate state purpose (like national security), and use the minimum restrictive means with procedural restraints against abuse. The ruling has clearly recognized national security as an acceptable concern to curtail the right to privacy, but has also warned that unless checked, unregulated powers by any surveillance agency will be disastrous to constitutional democracy. Even though Puttaswamy himself did not assess particular surveillance legislation, it made a constitutional requirement to the legislature to update and enhance interception systems. This requirement has been reiterated in subsequent judicial decisions, but detailed legislative reform does not exist.

Although privacy has been significantly entrenched in the constitution, the main laws on surveillance in India have remained subject to Indian Telegraph Act, 1885, which was formulated in the colonial era. Section 5(2) permits interception of messages in a public emergency or in the interest of public safety but these have not been defined and leave broad discretion on the part of the executive. The Supreme Court stated the procedural safeguards in People's Union for Civil Liberties (PUCL) v. Union of India (1997) that required interception orders to be overseen by committees and reasoned. But the ruling did not presuppose previous court approval, or even anticipate modern surveillance features like metadata aggregation, coded electronic communications, bulk surveillance devices, or automated software analysis. According to the scholars, the vocabulary of the Telegraph Act in the nineteenth century does not fit the twenty first century technologies hence a statutory mismatch that compromises the proportionality criteria that are required by Puttaswamy.

There is a parallel framework of surveillance authority in the Information Technology Act, 2000. Section 69 gives the government the power to intercept, spy on or decrypt information produced or transmitted across the computer resources, and Section 69A of the act gives the State the power to prevent online content. The provisions are operationalised into the Information Technology (Procedure and Safeguards the Interception, Monitoring and Decryption of the Information) Rules, 2009 and Information Technology (Procedure and Safeguards the Blocking of Access to the Information by Public) Rules, 2009. Within these guidelines, senior executive officials like Joint Secretaries have the ability to issue surveillance orders with post-facto oversight being done by review committees. It is important to note that the framework does not involve judicial endorsement at the warrant step, and the confidentiality of interception orders hinders transparency in society. It has been brought to attention by scholars and mass civil society organizations many times that the secrecy and generality of these powers poses a danger of disproportional, unaccountable and partisan surveillance. Procedural safeguards are further undermined by the lack of requirements to publish statistics and by the fact that there are few sources to which the affected person can appeal to find a solution. The latest in the Indian legal context is the Digital Personal Data Protection Act (DPDP Act), 2023, that attempts to formulate an overarching structure of the management of personal data. The Act brings forth rights of the data principal, responsibilities of the data fiduciary and the Data Protection Board with the role of monitoring compliance. Yet, Chapter V of the Act gives extensive exemptions to State agencies, based on such reasons as national security, domestic order and law enforcement. These exemptions enable the government to avoid fundamental data protection requirements including, however not limited to, a notice requirement, purpose limitation and storage conditions. Critics note that the scope of these exceptions, as well as the lack of autonomy of the Data Protection Board and pervasive central government authority to make rules, dilute the ability of the Act to have any significant privacy-protective effect. Even though the DPDP Act is a major step forward, it has been criticised as having a biased operationalisation of privacy provisions especially on the issues of national security.

In addition to laws, India has constructed a comprehensive surveillance and intelligence system that enhances the power of the State. Other systems including the National Intelligence grid (NATGRID) combine databases of various ministries and agencies of the government to facilitate real-time national security analytics. The Central Monitoring System (CMS) enablethe intelligence agencies direct access to telecommunications networks bypassing service providers, and this allows bulk interception. The Crime and Criminal Tracking Network System (CCTNS) and Inter-operable Criminal Justice System (ICJS) are the digital policing systems that ease the dissemination of biometric, criminal and demographic information among law enforcement organizations. The common application of facial recognition in policing, airport security, and surveillance of the population only increases the ability of the State to monitor and investigate people.Claims towards Pegasus spyware, which purportedly spies on journalists, activists and political figures, brought to light the danger of concealed and extremely advanced intrusions that had no legislative sanction or transparency to the public. The public findings were constrained despite a technical committee appointed by the Supreme Court to investigate despite deep rooted information lapses in transparency and institutional checks.

Collectively, the Indian legal and technological environment displays a surveillance regime typified by large-scale statutory authority, archaic legal practices, extensive national security privileges and the fast moving technological capacity. The fact that the constitutional norms are misaligned with the norms of the statutory practice highlights the necessity to introduce sweeping changes in order to make sure that the national security policies do not clash with the democratic values and the basic right to privacy.

CASE STUDIES AND EMPERICAL EVIDENCE

The empirical and investigative coverage can shed critical light on the functioning of the surveillance architecture in India in practice to understand the challenges posed between privacy and national security that the purely doctrinal discourses are incapable. Three case studies, such as the Pegasus spyware, interception and blocking orders through the statutory frameworks, and the National Intelligence Grid (NATGRID) provide an insight into the working reality of surveillance in India. They show how technological complexity, legal opaqueness and lax regulation all combine to form the privacy-security dynamic.

The 2021 Pegasus scandals are one of the most complicated and far-reaching surveillance scandals in Indian constitutional history. Pegasus which is an Israeli product of NSO Group is generally regarded as one of the most sophisticated spyware software in the world. Pegasus uses so-called zero click vulnerabilities, unlike traditional interception technologies, and thus can intrude into devices fully and without any trace of compromise of the target phone. This comes with access to messages, emails, passwords, location history, camera, microphone, encrypted communication applications. A global media consortium and forensic examination by the Security Lab of Amnesty International revealed that many Indian journalists, political strategists, lawyers, political activists, and political office-holders were potential and confirmed targets. The supposed targeting of those who were involved in dissent, investigative reporting or opposition politics posed the concern of the possibility of misuse of surveillance to suppress democratic participation.

The Indian government refused to confirm or deny that Pegasus had been acquired or put into service on the grounds of national security secrecy. This is what the Supreme Court of legal challenge was all about, namely, this official silence. The Court realised that the charges of possible hacking by state agents were serious and thus established an independent technical committee which was presided over by a retired Supreme Court judge. The proceedings of the committee, though disclosed less than even-handed collaboration with the government agencies and the issue of transparency and accountability. Although the

publicly published extracts of the final report indicated that evidence of Pegasus infection could not be determined with certainty in a number of the devices analyzed, The committee identified irregularities that were similar to indications of potential surveillance in India as well as highlighting deficiencies in the structure of the surveillance oversight frameworks in India. This brought up some basic legal issues- is covert hacking of devices ever justified by the legality and proportionality tests of Puttaswamy, are the tools used by such intrusion within the confines of the current interception laws, and is executive authorisation without judicial control constitutionally permissible? Pegasus proved that the current surveillance laws that were formulated in a time when the telephone tapping was the state of the art were ill placed to control very invasive digital spyware that has the capability to infringe upon rights on a massive scale.

A second example case is regarding the issue of interception and blocking orders in India that are being issued on a large scale by the Indian Telegraph Act and the Information Technology Act. There are no specific figures, as there is a statutory veil of secrecy, but parliamentary replies and other disclosures in RTI indicate that thousands of interception orders are made each year by the Union Government alone, and that state governments make additional orders. Censorship of online material, especially at times when civil unrest, protests, or communal tensions are eminent, has also taken a sharp upsurge. As an illustration, posts on these social media sites like Twitter, Facebook, and YouTube have often been censored or deleted under the directive of governments. In spite of the size of these orders, there is almost no transparency even interception orders are not announced, people are not informed, unless they are prosecuted, as well as the motives of their issue remain secret. Post-facto scrutiny is only subject to the review committees which are composed of senior executive officials and the executive remains in charge of both authorisation and oversight.

The secrecy of the interception and blocking orders raises a number of legal and constitutional issues. To begin with, as long as orders are not published or reviewed by the courts, the population cannot determine whether they fulfill the legality, necessity or proportionality requirements specified in PUCL and Puttaswamy.Second, it has accountability in secrets so that there is no one to answer to wrongful or politically motivated surveillance. Third, it means that people have insignificant channels of redress since they rarely know that their rights have been violated. Judicial action has been taken a few times, like to strike down blanket internet shutdowns or to compel them to disclose procedural safeguards; but these judicial interventions are spontaneous and fact-specific, and not structural. The weakness of the protections of privacy, where there is no independent authorisation and transparent reporting systems, is emphasised by the systemic power of the executive discretion.

The third case study, which is the National Intelligence Grid (NATGRID) and centralised data aggregation, provides an idea of how India is adopting massive, technology-based systems of intelligence without any legal regulation. NATGRID is programmed as a combined intelligence system that will interconnect various databases, including passport information, airline ticketing information, banking information, immigration information, driving licence information, and telecom information. It aims at allowing real-time access of information to security and intelligence agencies in order to counterterrorism and also to investigate.Although the use of a swift analysis based on data is quite reasonable when it comes to a national security issue, NATGRID casts significant privacy and civil liberties concerns. In contrast to most other intelligence systems in the world, NATGRID is not run by a specific statute by the Parliament. Rather, it operates based on executive discretion, without any specific legislative protection, without independent audit, without explicit retention and access policies. This gives rise to the fears of mission creep where a system designed to combat terrorism, slowly turns into a normal policing tool, political surveillance, or profiling of individuals or groups.

NATGRID risks are reinforced by parallel systems like Central Monitoring System (CMS), Crime and Criminal Tracking Network System (CCTNS) and Interoperable Criminal Justice System (ICJS) that cumulatively increase the capability of the State to collect, cross-reference and analyse sensitive personal data at an unprecedented level. Such systems can optimize investigative efficiency, although without legal restrictions, can be used to conduct mass surveillance, discrimination on the lines of profiling, and violation of data protection standards. The civil society organisations have continuously pointed out that the centralized intelligence platforms should be parliamentarily accountable, their operations are guided by clear operation policies, and that their data protection measures should be strong, which is not the case. Collectively, these case studies demonstrate a very similar trend the ecosystem of surveillance in India is growing at a high rate in terms of both technological capability and institutions, yet the legal framework and the oversight architecture have failed to keep pace. The consequences are that it will create a lot of gaps in transparency, chances of random or politically inclined surveillance and the risk of breaching the basic right of privacy.

ANALYSIS: KEY TENSIONS AND PROBLEMS

The modern Indian surveillance and privacy legal framework is an incomprehensible maze of unresolved legal tensions, structural gaps and emerging technological issues that all interact to form the interaction between privacy rights and national security. The root of this tension is in the legal structure, where the State has much power, and individuals have few substantive protections. The initial large fault line is the breadth and ambiguity of the statutes in India regarding surveillance. Even the laws like the Indian Telegraph Act, 1885 and the Information Technology Act, 2000 still use such age old and undefined terms like public safety and public emergency. These words were introduced in a colonial setting which aims at containing political dissent, and not dealing with contemporary security threats. Their ambiguity has given state authorities the opportunity to read them in a broad way such that the reasons behind surveillance could extend way beyond what would be considered proportional by current standards. The doctrinal conditions of the Puttaswamy judgment such as legality, necessity, and proportionality require specifics in the laws granted to a right limitation. However the existing laws lack specifics in their criteria, specific conditions of authorisation, as well as situation specific restrictions applicable to digital ecosystems. This results in an extensive discretionary space in executive agencies which have created the potential to have an expansive understanding of national security that borders on normalising everyday and ubiquitous surveillance in contexts which are not extraordinary by any means.

Strongly connected with the scope of these powers is the vulnerability of procedural protection of interception and monitoring. Interception orders in jurisdictions that have strong privacy rules must be pre authorized by an independent vested court or other special courts. In striking contrast, the system of India is largely that which centralizes the authority to make authorisation decisions in senior executive officials, who are usually the Joint Secretaries. Even the review committees that are supposed to be oversight institutions are composed mostly of the members of the same executive departments that present the surveillance requests. This puts an intrinsic conflict of interest which compromises the independence and objectivity of the essential meaning of checks and balances. Lack of judicial review indicates the issue of rubber-stamping of requests and allows regular approvals without strict evaluation of necessity and proportionality. Furthermore, the statutory mechanisms to inform people once the surveillance is completed do not exist even in those instances when the interception was wrongful or disproportionate. This absence of responsibility is further enhanced by the fact that orders are shrouded in complete secrecy making them beyond open debate, parliamentary scrutiny and even academic criticism. Consequently, legal protection is not as a substantive check but rather an administrative formality that can be easily abused or overexerted.

The other significant point of tension can be seen through the wide exemptions of the State established by Digital Personal Data Protection (DPDP) Act, 2023. Although the Act represents a groundbreaking development since it offers a statutory framework on data protection, its structure is widely ridden with carve-outs of government agencies. The State can waive core data protection requirements, including consent, purpose limitation, storage limitation and transparency requirements, where any type of activity is undertaken by the State in the interests of national security or in the interests of public order or in the interests of investigative activities. These provisions resemble the imprecise and loose-defined language of previous laws, which allows blanket exemptions in the face of possibly unprotected mass surveillance. Since the Act does not require an independent monitoring or judicial authorisation of access to personal data by state, the exemption framework threatens to wash away mass surveillance activities. Moreover, the Data Protection Board, the enforcing authority, lacks the institutional autonomy of international bodies relating to data protection. It lacks capacity to investigate or question state surveillance programmes, and its limited power and mandate makes this impossible. Therefore, the exemption framework of the DPDP Act undermines the privacy-security balance by making it institutionalised executive control of the data management.

The further complexity has been brought about by technological development given the fact that the legal frameworks of India have not evolved as much as the surveillance technologies that are fast being formed.Pegasus spyware, facial recognition, predictive policing algorithms, and analytics that use artificial intelligence have radically changed the character of state surveillance. In contrast to the old-fashioned wiretapping, the contemporary surveillance means enable one to access the encrypted communication, metadata trends, location logs, biometric identifiers, and behavioural cues at a greater level as well as accuracy than ever. The Indian legal framework, nevertheless, is still based on the ideas developed in the voice telegraphy of the analogue era. It is the result of this disparity that the State can use intrusive technologies in a legal vacuum, with no particular statutory authorisation, judicial oversight, or elaborate data-protection measures. The Pegasus scandal proves that even advanced surveillance instruments can bypass the procedural protection, including interception approvals, as they do not imply interception of communication but hacking of devices. Likewise, police and other investigative agencies that utilize facial recognition technologies tend to run without legal provisions that regulate accuracy, bias testing, retention, and misidentification rights of contesting. The growing technological potential of the State without revised laws will threaten to establish a situation in which surveillance becomes ubiquitous, programmed, and unnoticeable, and therefore undermines constitutional protections.

The issue of national security inquiry becomes even more complicated where the scope of investigation and flow of data across borders interconnect. Global technology firms with headquarters out of India store a large percentage of the information they could be pertinent to security investigations. The availability of this type of data relies on Mutual Legal Assistance Treaty (MLAT) systems, which are cumbersome, time-consuming, and in many cases, cannot be effectively deployed to the expediency of counter-terrorism or cybercrime investigations. India has no formalized Standard Operating Procedures in seeking the data of foreign parties and the world systems are regulated by disordered compliance strategies imparted by their home authorities. This poses a two-fold challenge, as security operations will be delayed, which can impair investigations, and the protection of privacy when foreign actors act differently or arbitrarily. Lack of harmonised data-sharing regulations, data localisation protection and cross-border responsibility systems leads to legal grey areas whereby no privacy or security is provided. The executive agencies will have the temptation of using informal channels or pressure tactics to get data in this vacuum and this brings the concern of due process.

A different developing tension is the increased involvement of the vendors in the industry of surveillance in providing advanced equipment to the government. There are no transparent procurement standards, disclosure procedures and mandatory cybersecurity audits that companies building spyware, analytics systems, biometric solutions and AI-driven surveillance technologies are bound to. Because of this, the citizens do not know which tools are utilized to track them, the contractual provisions to safeguard the processing of the data, and the standards to hold the vendors accountable. The obscurity of the procurement procedures is also a reason to increase the corruption risk and inability to ensure that tools meet the constitutional requirements. More so, the private vendors are usually transnational, which casts the doubt of foreign influence, data security and a possible backdoor vulnerability. Lack of rigorous due-diligence frameworks, independent audit, and procurement transparency means that integration of the private actors into the national security architecture forms an unregulated surveillance ecosystem that is locked out of democratic scrutiny.

Lastly, the enforcement of compulsory digital ecosystems has led to the erosion of meaning consent albeit subtly. With the administration, welfare provision, medical services, and financial services digitizing, citizens are finding themselves in scenarios where they are unable to access the much needed services unless they submit personal information. Compulsory applications, databases of welfare, and firmware that comes pre-installed on devices, which is enabling surveillance, form a space in which people could not make authentic choices. This is a manipulated agreement that weakens the freedom of choice that is involved in the right to privacy and justifies the wide-range of data gathered by the state in the guise of providing services to the people. Combining different databases also increases the likelihood of function creep, where welfare administration systems are used to do policing or intelligence without legislative authorization. This erosion of the distinction between the governance and surveillance enhances the ability of the State to spy on citizens at all times, in an insidious transition to the data-driven security approach in India that is not debated or regulated by law.

RESEARCH GAPS AND EMERGING PROBLEMS

The privacy environment in India after 2017 presents some of the emerging research gaps that are not well filled even as the available constitutional and policy literature continues to increase. There is a big gap in the lack of a mapping of surveillance practices through empirical oversight. Despite widespread exercising of the interception, monitoring, and blocking powers by central and state agencies, such a high level of secrecy of the authorisation procedures has resulted in the lack of any consolidated public data as to the amount, nature, and rationale of such orders. Thus, it is still true that scholarship is limited by conjecture, anecdotal revelations, and disparate RTI reactions. There are no formal reporting or independent audit requirements to determine whether surveillance orders are of such necessity, proportion or legality as to comply with constitutional standards, or whether they are disproportionately targeted against journalists, activists, minority groups or political dissidents. Second, the absence of impact assessments of mass data aggregation systems, such as NATGRID, CCTNS, ICJS, and large-scale welfare databases, is almost complete. Although such systems are reasonable in the context of national security and effective investigation, there are practically no empirical studies on the effectiveness of their work.Scholars do not have access to performance measures like increases in investigative timelines, correctness of information correlations, false positive rates or quantifiable contributions to counterterrorism outcomes.The absence of such evidence does not allow concluding whether the intrusion created by mass aggregation is reasonable or whether some less intrusive measures are possible that would produce the same results.Third, academic criticism has lagged behind AI-based surveillance systems, which have have since increased in size (facial recognition systems, predictive policing algorithms, behavioural analytics, and automated social media surveillance).

Indian research has not comprehensively examined the concept of algorithmic bias, discriminatory results, the fact that the rate of errors varies between one population and another, or that the marginalized populations may be profiled.

According to global studies, structural inequalities are frequently copied by such systems and feedback loops are formed but the application of AI tools by law enforcement agencies has not been properly documented in Indian scholarship. Moreover, the fact that there are no statutory mechanisms that regulate automated decision-making or algorithmic transparency only increases the dangers of opaque and unquestionable state action. Fourth, the scandal involving Pegasus spyware depicts profound lapses in the comprehension of the acquisition, control, and management of spyware. The veil of secrecy of the surveillance technology markets is the fact that the researchers can never see the procurement procedures, vendor history, contractual protection, security audit, and regulatory verification of acquiring extremely intrusive cyber tools. In addition, there is virtually no literature on the legal standards, should any, exist in approving such tools, the methods by which judicial review may be sought, or the remedies that may be available to the victims of illegal usage of unlawful spyware. This is a particularly grave gap as sophisticated spyware allows zero-click attacks that do not adhere to any statutory interception system whatsoever, which creates some fundamental constitutional questions that have not been exhaustively investigated. Fifth, there is a tremendous lapse in terms of cross-border data access, DPDP Act exemptions, and MLAT processes due to the increasing dependence of India on global cloud platforms and other foreign service providers. Encrypted data or offshore data is often needed by national security investigations, but there are no harmonised systems of mutual legal assistance between India and other countries, the pace of diplomatic processes is slow, and there is no alignment with international regimes of mutual legal assistance like the US CLOUD Act or EU e-Evidence regime, which contributes to long delays and uncertainties. The effects of exemptions in the DPDP Act, especially in allowing unrestricted processing of personal data in the name of national security, on the norm of cross-border transfers, cross-border foreign data protection legislation, or the platform-imposed compliance requirements have not been fully investigated in the academic literature. Without such research, the policymakers will have no clear advice on how the cross border data governance architecture in India should be reformed. Lastly, a new but under-researched field of interest is the privacy question of compulsory app ecosystems and device-level digital requirements. The rapid implementation of government-suggested apps, namely, the most notable one during the COVID-19 pandemic, Aarogya Setu, reveals unanswered questions regarding voluntariness, consent, data storage, secondary use, and the long-term management of the information gathered. Whether the volumes of data required by such apps justify their claimed public health or administrative objectives, whether consent in mandatory systems is actually meaningful, or how such digital infrastructures can become the permanent surveillance vectors even after their original objective is achieved, is under-researched. Also, compulsory digital interfaces may disenfranchise people who do not have access to smartphones or literacy, yet the exclusionary or discriminatory effects of these systems have not sufficiently been studied by Indian scholarship. All of these emerging gaps reveal that constitutional privacy jurisprudence in India is highly developed, but the empirical, technological and operation aspects of interactions between privacy and security are insufficiently studied.To fill these gaps, interdisciplinary collaborative efforts, including (but not limited to) the legal literature and empirical social science, cybersecurity research literature, technology studies, and international comparative analysis, will be required. Devoid of such thorough investigation, India will have a chance of developing national security policies that are technologically backward, constitutionally weak, and lack the necessary theoretical basis in evidence-based review.

PROPOSED SOLUTIONS AND POLICY RECOMMENDATIONS

In finding a solution to the enduring conflict between privacy rights and national security in India, there is a need to take a multi-pronged legal, technological and procedural reform approach. The most basic and primary recommendation is the legal redrafting and limitation of the surveillance authority. The existing law, such as the Indian Telegraph Act, 1885, and parts of the Information Technology Act, 2000, is based on very wide and vaguely defined terms like the one of public emergency and the one of public safety, providing the executive with too much discretion. These outdated provisions need to be substituted by a complete Surveillance Reform Act that provides a clear definition of major concepts, defines the allowable extent of surveillance, and directly incorporates tests of proportionality and necessity into the Statute. This legislation must also create a distinction between regular intelligence collection and high-risk surveillance activities, and the laws should be more serious on the elements of intrusive tools. Modernisation of the statutory framework will allow India to lessen the grey area, the powers of national security to be consistent with constitutional protections and to create predictable legal principles by which the agencies should operate, which in turn can enhance accountability and citizen confidence.

To supplement the statutory reform, it is necessary to introduce high-risk surveillance, which must be carried out by the court or another independent body. Such practices as device hacking, installation of spyware, decryption of communications on a mass scale, or massive aggregation of metadata are invasive types of surveillance that can result in extreme privacy violations. In these instances, the pre-judicial authorities must be obligatory, or at least permission must be sought by a third party quasi-judicial body that would be completely independent of the executive branch. The move would establish a much-needed control over arbitrary action and make sure that the proportionality and necessity concepts codified in the Puttaswamy ruling find their way into practice. Such a system may mimic international solutions, such as the so-called dual lock in the Investigatory Powers Act of the UK, in which high-risk interception warrants must not only be approved by an executive in that case an independent judge, but it also offers procedural rigour and accountability.

Complementary is the pillar of reform of having independent checks and balances in place. A separate Surveillance Oversight Commission must be given the powers to engage in thorough audits on the intelligence and law enforcement agencies, as well as to examine allegations of illegal surveillance, and release redacted annual reports to ensure accountability to the citizens. The powers of the commission should possess the capability to enforce the adherence of the statutory protections, suggest the remedial steps, and oversee the execution of Data Protection Impact Assessment (DPIAs) of surveillance programmes organized by government. Independence of institution, legal power and public disclosure are essential in ensuring that the oversight is not just symbolic but substantive and as such, the obscurity that has characterised the surveillance ecosystem in India, is reduced.

Moreover, it is important to enhance the protection of the DPDP Act to avoid over intrusion in the name of national security. The existing exemptions are too broad so that the State can obtain consent, limit purpose, and transparency requirements. Reduction of such exemptions, regular reviews and the statutory designation that all high risk surveillance programmes receive the obligatory DPIA will establish a balanced countermeasures between security demands and individual rights. Where feasible DPIAs must be publicly summarised without disclosing any sensitive operational information so as to increase transparency and promote responsible decision-making.

Another non-negotiable aspect is a transparent procurement process and accountability of the vendors. The recent case with the spyware like Pegasus shows how dangerous it is when the procurement is opaque and the vendors are not

checked. All surveillance technologies must be purchased in transparent and open and audited procedures. Technical audits, human rights due diligence procedures, and legal contractual safeguards ought to be compulsory to make sure vendors follow the security, ethical, and constitutional norms. Procurement transparency does not only reduce the chances of misuse but also provides a chain of responsibility which is necessary to be accountable in the event of misuse or malfunction.

Technologically, intelligence can be facilitated by the promotion of privacy-saving measures that will promote the pursuance of intelligence without leading to violation of fundamental rights. Analysis of patterns and threats with minimum direct-exposure of individual data can be achieved through end-to-end encryption, differential privacy, federated learning, anonymisation and other sophisticated data-protection techniques. The implementation of these technologies promotes national security innovation and respect constitutional assurances and minimizes the use of blanket data harvesting methods. It is also essential to make available solutions to unlawful surveillance. Privacy violations should be seen as a harmed operation in courts that would allow individuals who experienced it to be compensated. There should be mechanisms to challenge such as the public interest litigation and specialised tribunals to ensure that individuals who have fallen victims of unlawful interception or data misuse have access to such mechanisms. The availability of remedies strengthens the shield effect against the overreach, and creates an indication that the State is answerable and offers victims real redress.

Capacity building and judicial training is also important in the successful implementation of these reforms. They need to sensitise judges, investigators, and policymakers to the emerging technologies, the complexity of AI and algorithmic surveillance, cybersecurity, and constitutional standards. The institutional competency will be improved by specialized benches of cyber-law and the continued training program of law enforcement officers and judicial officials will allow them to make informed decisions and properly interpret the complicated cases of surveillance.

Lastly, enhanced international collaboration is required in a globalised world where the flows of data and globalised technology platforms are transnational. To ensure that cross-border data access procedures are in tune with international standards, simplify MLAT processes, and participate in conventions like the Budapest Convention on Cybercrime, India should harmonize cross-border data access procedures with international standards and simplify the MLAT processes. The transnational cooperation will help secure the legal and respective access to the information which is stored abroad, meet the international human rights standards and minimize the use of the extrajudicial methods which may lead to the invasion of privacy.

These recommendations combined provide a rights-compatible surveillance ecosystem. The resolution of the issue of balancing the needs of national security and the constitutional privacy protection can be achieved through statutory reform, judicial authorisation, independent oversight, enhanced DPDP protections, transparent procurement, privacy saving technologies, remedies in the event of violations, building capacity and cooperative efforts across national boundaries. Through such a multi-layered approach, India can be assured that her surveillance system functions within the confines of law, proportionality and accountability, and it will become a beacon of the world in terms of democratic and rights-sensitive intelligence governance.

CONCLUSION

Though this paper is a legal/policy analysis of privacy rights and national security interplay in India, it recognizes various structural constraints which influence the level and extent of study. The number one restriction to these is the nature of confidentiality of the national security operations which seriously limits access to the primary data. The detailed details

on interception orders, surveillance, the use of spyware or the internal operations of intelligence systems like NATGRID and the Central Monitoring System (CMS) are mostly secret. Even under the provisions of the laws, like the Right to Information (RTI) Act, any disclosures are not comprehensive, timely or uncensored and it is difficult to empirically test the extent, rate, and volume of surveillance. Likewise academic studies on high-tech surveillance techniques such as AI-based analytics, facial recognition, predictive policing and undercover spyware have barriers in the form of non-disclosure deals, secret procurement deals, and insufficient technical transparency. Consequently, research tends to use secondary reports, media research or country of case studies which although informative, may not be a complete representation of the reality of how the intelligence infrastructure is being performed in India. Also, the comparative frameworks, though beneficial in determining the best practices, should be used cautiously. Models like the EU General Data Protection Regulation (GDPR), the United Kingdom Investigatory Powers Act, or the FISA reforms of the United States of America are in legal, political, and institutional environments that are vastly dissimilar to the situation in India in constitutional and administrative terms. These mechanisms cannot be directly transplanted or this is not always the right thing to do. Consequently, the global comparisons of policy recommendations need to be contextualized to suit Indian needs, and technology, legal, and security needs must be balanced in accordance with global norms. The nature of technology is also another limitation since technology is dynamic. Surveillance technologies, artificial intelligence, and data compilation software evolve fast, and they sometimes go ahead of legislation and supervisory systems. As a result, any policy or legal analysis is a time-dependent phenomenon that might require revision constantly to be applicable and efficient.

Although this was limiting, the paper highlights that the status of privacy as a basic right is a constitutional requirement as well as a pillar of democratic governance. The comparison shows that the current legal system in India is inconsistent, based on old laws, and not well-adjusted with the current technological facts. Wide statutory wording, discretionary executive authority, weak procedural protections, limited transparency and opaque procurement procedures all lead to structural vulnerabilities that have the potential to violate privacy and offer a partially functional system of national security. The complexities are exacerbated by the emerging technologies, aggregate data of masses, surveillance with AI, and the obligatory digital ecosystems that increase the risks of misuse without appropriate legal and institutional regulators.

The solutions to these gaps discussed through this paper are the recommendations that are expected to fill these gaps. Accountability can be enhanced through statutory restructuring, judicial or independent pre-emptive consent and the creation of independent supervisory institutions to provide that intrusive powers are used in the appropriate manner. Restricting the exemptions in DPDP Act, requiring Data Protection Impact Assessments, and incorporating privacy-preserving technology (initially) will lead to providing better protection to the rights of individuals and ensuring the efficiency of the operations. Open procurement procedures, accountability of vendors, and easy access to redress of unlawful surveillance are some of that enhance institutional integrity. Moreover, enhanced global collaboration, and equalised cross-border data access systems enhance effectiveness of national security operations within the globalised digital space.

Finally, a surveillance ecosystem that is consistent with constitutional privacy rights will not undermine national security, but rather increase legitimacy, trust among the population, and effectiveness of operations. Incorporating privacy-aware software in the laws and the policy framework of India, thus, is not only a normative task but also a strategic requirement. A balance between privacy and national security is the key to the continuation of democratic governance, upholding individual freedoms, and strengthening the legitimacy of state institutions in a world where India

will face multifaceted digital, geopolitical, and security issues. The future strength of Indian democracy thrives on the effective incorporation of the sound legal protections, responsible institutions, and technology-intensive security systems into a coherent system of rights-abiding surveillance.

*****