IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SURVEILLANCE VS. PRIVACY: BALANCING NATIONAL SECURITY AND INDIVIDUAL RIGHTS IN INDIA

SIDHARTH

LL.M Student

Roll Number: 230906262013

Amrit Law College,

Veer Madho Singh Bhandari Uttarakhand Technical University, (Uttarakhand)

Abstract: Any critical and nuanced analysis of what contours this discourse – security versus liberty – must begin by placing it within the legal and socio-political context of India. Inspired by the evolutionary laws of Great Britain, India inherited a complex regime of surveillance through the Information Technology Act 2000, and the Indian Telegraph Act 1885. The advent of the technological revolution has led to the use of various surveillance architecture like Aadhaar (unique biometric ID), centralized monitoring systems (CMS), air traffic surveillance (NETRA) and national intelligence grid (NATGRID), all of which have in turn, like everywhere else in the world, created concerns about safety and security on the one hand, and the right to privacy on the other. The recent judgment by the Supreme Court in the Aadhaar case, Justice K S Puttaswamy (Retd) v. Union of India, recognized privacy as a fundamental right. The judgment talks about the need for 'proportionality, legality and necessity of state action' that can be bring used to bring about a violation to an individual's right to privacy. Thus, the discourse of surveillance oscillates across time, across evolving legal regimes, and is situated squarely on the idea of the tension between surveillance to ensure freedom and surveillance to ensure guardedness. The fluidity with which India intends to keep changing and creating laws related to privacy and data protection can be seen in the passage and discussion of the personal data protection bill, which acknowledges the tension between the demand for the need to ensure security and surveillance and the need to also uphold the right to privacy within the democratic legal framework.

Keywords: - Surveillance, Privacy, National Security, India, Information Technology Act Aadhaar, NETRA, NATGRID

Introduction

A transnational dialogue on spying over safety or surveillance versus privacy is underway all around, and anxieties over national security and civil liberties are all the rage. The Indian variation on this theme, however, has its own distinctive cadence. This has as much to do with the raw numbers, its pluralistic culture and the nature of its democratic ethos. The maze of surveillance in India is made up of the cascading obstacles built up by law, technology and the judiciary, and this fabric embraces the most intimate ideas of personal privacy, as well as the most intrusive notions of aggressive national security.

India has a complex surveillance regulatory framework, comprising a set of statutes authorizing interception and surveillance, such as the Information Technology (IT) Act, 2000, and the Indian Telegraph Act, 1885, as well as a slew of rules and policies that codify the broader contours within which state as well as non-state actors can undertake surveillance. For instance, the IT Act, 2000 authorizes the 'interception, monitoring or decryption' of information, revealing that India is awakening to the legal challenge of technologies.

Furthermore, the Indian state has relied on various kinds of digital surveillance – from biometric archives such as Aadhaar to mass digital surveillance architectures like the Central Monitoring System (CMS), network traffic analysis (NETRA) and the National Intelligence Grid (NATGRID) – to aggregate, collate and process data in bulk for the purposes of securitization, governance and administration. Nevertheless, these authorization technologies, once they're in use, have triggered fears of privacy. Take the Aadhaar system, an effort to assign every Indian resident a unique identifier, which has generated several controversies related to privacy and privacy abuse. Embedding privacy as a basic right in the Constitution of India, the country's 'privacy judgment' – i.e., the verdict in Justice K S Puttaswamy (Retd) v. Union of India – by the Indian Supreme Court is central to the present debate about what kinds of privacy rights exist in India. In that judgment, the court observed that privacy forms part of 'personal liberty … which shall be protected as a matter of right against any infringement by any authority … children have a right to privacy that can be protected against arbitrary or unlawful State interference … and protections including the doctrines of 'proportionality' and 'procedural guarantees' – the principle that any such interference must be 'lawful', 'reasonable' and 'proportionate'.

The need to balance the interests of national security with the safeguarding of the rights of individual privacy arises because of the fundamental values of democracy and the rule of law. Among them, the security of the state – the sovereignty and territorial integrity of the state and, ultimately, the vital interest of its citizens – is paramount. If the state's self-interest is the first, the state would wish to retain its authority and to control the conduct of those on its territory. Surveillance is an instrument that states use to anticipate challenges to their authority, to engage in counter-terrorism activities, and to maintain general security and public order. The collective benefits of security can be important in the face of serious threats to society. Secret police pursuing its work without restraint can lead to what has been called a surveillance state, leading to the loss of many civil rights and liberties.

So, the challenge is to make sure that any surveillance apparatus is used judiciously, with effective oversight and control that should serve to check the abuse of power. Proportionality dictates, for example, that any act of infringement to an individual right on the basis of surveillance should be necessary, sufficient, least

burdensome, and always reviewable by the courts. Hopefully, the tension between two possible outcomes, a more despotic state that ignores the rule of law, or one that risks sacrificing security and police capability because of mistrust in government institutions, will always stay alive. Policing public space will inevitably take many years to learn the new value placed on privacy. The curtailment of rights or liberties arising from the mass-surveillance systems now becoming prevalent will be matched by significant new security risks for governments that dare to be more public in their management of private spaces – particularly if markets and tackling the financial crisis are their main concern. Much depends on the extent of our capacity for collective action and solidarity – one of the ingredients of a genuine democratic ethos – which, paradoxically, will have to withstand the pride that governments may have at monitoring and measuring private spaces.

Further, we need to constantly update and review the statutory framework governing surveillance and privacy to remain abreast with technological advancements – the Personal Data Protection Bill is an important step in the right direction, once it is passed, as its objectives include the establishment of a data protection authority, establish mechanisms for data protection and privacy, and enumerate the rights of individuals with respect to personal data.

Historical Context and Evolution of Surveillance in India

The history of surveillance in India is a story flowing through the precolonial, colonial and postcolonial eras, and it's transformed across the centuries with the passage of historical technology and political societies. This historical saga of the evolution of surveillance – from simple techniques to sophisticated digital surveillance – covers a vast array of techniques, legislation and processes that reflect an uneasy mix of state power, right and the interests of privacy.

Early Surveillance Practices and Their Legal Bases

In pre-independence India, surveillance was a colonial regime's tool for both discipline and control. The British Raj put in place laws and measures to implement surveillance to quash anti-colonial agitations and move towards denial of any space for civil liberties. The Indian Telegraph Act of 1885 was the first piece of legislation instituting the right of government to intercept telegraph messages for the maintenance of 'public safety', a legal foundation for state surveillance to take hold.

Other than the interception, the yoke of surveillance involved extensive, physical surveillance, such as informers, spies and agents, especially the subversive elements that posed threats to the British crown – i.e., the freedom fighters and the political leaders spreading the agenda of independent India. These early applications of the surveillance techniques were driven by colonial interests, operating under the legal and institutional frameworks that promoted the centralized powers of the Indian colony under the state of colonial rule.

Post-independence Developments in Surveillance for National Security

The colonial legacy of surveillance was handed over to the newly installed democratic government of independent India. The early postindependence years were marked by the retention and modification of the colonial-era laws for the neo-colonial period, with a broad emphasis on national security and territorial integrity. In this context, the Indian Telegraph Act of 1885 has continued to serve as the key legal instrument

through which the independent Indian government has sought to monitor and intercept communication 'in the interests of … national security.

Alongside this transformation in technology, immediate backlash of the post-independence period also saw a new raft of laws and amendments to existing laws, as nations adapted their legal infrastructure to the realities and pressures of the modern nation-state. For instance, the Official Secrets Act (1923) – previously enacted during colonial rule to suppress revolutionaries and nationalist movements – was retained by new governments and used to prosecute spies and protect state secrets. However, heated debates about the need for oversight of these laws and protections for individual rights laid the foundations for future legal and policy battles over surveillance.

The Evolution of Digital Surveillance in the 21st Century

The digital age brought about an especially dramatic revolution in the history of surveillance in India. With the introduction of the Information Technology (IT) Act, 2000, the law began to catch up with the new potential and reality of electronic surveillance, which was brought about by the internet and mobile telephone revolution. The IT Act covered areas such as the 'legal recognition of electronic records', 'digital signatures and 'cybercrime', among others, charting the course for modern methods of surveillance.

Alongside extreme communal violence and the institutionalization of caste, the first years of the 21st century have witnessed more ordinary forms of Indian state invasion of privacy, through the erection and gradual implementation of large-scale digital surveillance projects — from the biometric Aadhaar database, to the Central Monitoring System (CMS), to the National Intelligence Grid (NATGRID), and the Network Traffic Analysis (NETRA) programme, all attempting to leverage technology to serve the state in making more effective decisions about governance, security and service delivery. In doing so, from the very beginning they have provoked intense domestic and judicial pushback regarding privacy.

However, the judgment in Justice K S Puttaswamy (Retd) v. Union of India triggered an important turn. It declared privacy as a fundamental right under the Indian constitution. This judicial declaration, made by the Supreme Court in 2017, has since led to an intense debate about the ideals, legality and desirability of digital surveillance.

The history of surveillance in India illustrates how India developed colonial regulatory mechanisms to modern digital surveillance through legislation that has continuously adapted to new challenges and technologies. It is a continuum rather than breaks. This historical perspective puts the present 'surveillance vs privacy' debates in the Indian context and provides a balanced perspective on finding the right approach to push for national security where vital interests of the state need to be protected, but at the same time safeguard the rights of the individual. It is desirable for India to calibrate a nuanced framework, with lessons drawn from its history and the principle of democracy, rule of law and respect for individual rights. There is no one universal approach to the complexities of the surveillance and privacy relationship in the digital age. Moreover, as Thomas Hobbes teaches us in his Leviathan, it is the security of life and property that is most desired by a people. For a democratic country like India, the state needs the power to provide that security for individuals if it wishes to survive. In the ever-evolving world of technology with potential for misuse, India needs to definitively

figure out the extent of surveillance, while simultaneously addressing the grievances of those who challenge it.

Legal Framework Governing Surveillance in India

The juridical scaffold that enables surveillance in India is a hodgepodge of colonial-era statutes and contemporary legislation, combined with landmark judicial precedents, through which the state's security imperatives must be balanced against the sanctity of individual rights. These tensions play out with increasing frequency, and with technological and cultural change.

Constitution of India: Fundamental Rights and Privacy

The Constitution of India, the supreme law of the nation, contains a number of fundamental rights that protect the civil liberties of the people of India. While the right to privacy itself does not form part of the Constitution, the country's Supreme Court has, through prior case law, repeatedly clarified that privacy is an integral part of the right to life and liberty under Article 21 of the Constitution.

In the landmark judgment in Justice K S Puttaswamy (Retd.) v. Union of India, the right to privacy was finally established as a fundamental right, implicitly affirming the constitutional status of individual autonomy, bodily integrity and personal decision-making. The judgment also set up a precedent for subjecting all current and future surveillance measures to the bar of privacy rights.

Article 21 and the Right to Privacy

The right to life and personal liberty guaranteed under Article 21 of the Constitution is a 'protean right', under whose shelter all facets of the right to privacy have been carefully nurtured and cultivated by the judiciary. The broad nature of this provision received a significant gloss in 2017 after the Supreme Court in Puttaswamy judgment defined privacy to embrace any invasion of one's personal sphere that passed a three-pronged test: one, that the law prescribing such an invasion be law for want of anything better; two, that such a law needed to be 'necessary' for the 'legitimate' aim sought to be achieved; and three, that such law needed to be proportionate such that the means chosen to achieve the ends were not vehemently disproportionate. This test is now the blueprint for checking the constitutional validity of any surveillance operation.

Information Technology Act, 2000: Provisions for Digital Surveillance and Data Protection

The Information Technology (IT) Act, 2000, is one of the key legislations pertaining to digital surveillance. It acts as the statute enabling electronic governance, regulatory framework of cyber activities, and provisions based on digital privacy and security. Accordingly, the provisions of the IT Act specify that the central government, or any of its officers authorized by the government may: (i) intercept, monitor or decrypt or cause to be intercepted, monitored or decrypted any information generated, transmitted, received or stored in any computer resource; or (ii) restrict access to any computer resource; in the interest of sovereignty and integrity of India, defense of India, security of the state, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence. This can only be done if there is prior approval granted under the rule-making process specified in Section 85 of the IT Act, 2000. Notification under these rules is subject to ' reasonable cause and cannot be made merely on the basis of generalized suspicion'. Data intermediaries such as Airtel, Facebook, Twitter

and LinkedIn all share the duty as per Section 85(5) necessary to ensure adherence to the orders. The provisions are ill defined and lack procedural safeguards and oversight mechanisms Section 69 of the IT Act, 2000 along with Sections 69A and 69B are the main legislations concerning digital surveillance. All these provisions of the IT Act can be applied by the government for the interests of the sovereignty and integrity of India, defense of India, security of the state, friendly relations with foreign States and public order.

The Telegraph Act, 1885, and The Indian Post Office Act, 1898: Surveillance of Communications

In the late 19th century, the Indian Telegraph Act of 1885 and The Indian Post Office Act of 1898 were enacted, followed by the Indian Wireless Telegraphy Act of 1933. These are the oldest legislations in India that govern communication surveillance. The telegraph Act allows the government to intercept telegraphic messages for the purposes of preserving sovereignty or integrity of India, the defense of India, friendly relations with foreign states, or public order. The Post Office Act allows the interception of postal articles for broadly similar purposes. These Acts were devised for the pre-digital era but applied to the modern world, with newer interpretations every time the law was challenged in the courts. There have been increasing voices calling for greater modernization of the archaic legislation to better protect the Indian citizens' rights to privacy in the era of digital communication.

The Aadhaar Act, 2016: Biometric Data and Privacy Concerns

The objective of the Aadhaar Act, 2016, which stands as the statutory basis for Aadhaar, is laid out in its long title: An Act to provide for the creation of a unique identity authority for issuing unique identity numbers to residents for establishment of their identity; and for matters incidental thereto or connected therewith. When we read statements like 'last week's financial support from the state will land in your bank account next week, provided the job center has your Aadhaar number', we understand that Aadhaar aims to enable 'targeted delivery' of financial and other subsidies, benefits and services. It's not difficult to recognize Aadhaar as a milestone project in India's emerging programme of digital governance. However, because of privacy risks associated with the collection, storage and use of biometric data, particularly in the Aadhaar with measures that can adequately protect the privacy of Indians who are required to surrender their biometric data and hand them over to the state?

The contours of the legal framework for surveillance in India, then, is a complex web of constitutional principles, statutory provisions and judicial graces, as the courts and the legislature skirt between the twin and often competing goals of securing the state's interests on the one hand, and upholding the rights of the individual, on the other. With technology further complicating the quest for a balance, the debate between surveillance and privacy, complete with judicial oversight and legislative action, is a dynamic space that speaks of a healthy democracy that is on its way to calibrating its constitutional scheme and institutional arrangements to the ideals of liberty, dignity and security. The story of the legal journey is unlikely to end here. It remains one of constitutionalism's triumphs over the imperatives of national security.

Digital Personal Data Protection Act, 2023: Implications for surveillance and privacy

A step in the right direction is the Digital Personal Data Protection Act, 2023 (DPDP Act) introduced in India this year, with the aim of protecting the 'right to privacy' of individuals in the digital age and refraining from unreasonable surveillance. The DPDP Act provides a broad and new framework for personal data processing

and gives Rights and Obligations to two parties (called a Designated Authority), the Data Principal (individuals) and the Data Fiduciary. Here are the key implications of the Act for surveillance and privacy.

Rights and Obligations

- Rights of data principals: Data principals have a right to know the information processed about them and if this information is wrong, to have it corrected, as well as deleted if deemed inappropriate, they have the right to name a person who can exercise these rights if they are dead or not of sound mind; they can complain to the public grievance redressal authority; they can withdraw consent at any time.
- Obligations of Data Fiduciaries: Anyone processing data is obligated to do so with express consent, keep data accurate and up to date, safeguard data, respond to attempts by the Data Principal to claim their data, inform the Data Principals of a breach, and erase data once its purpose has been fulfilled. (Note: Obligations of 'data fiduciaries' are omitted for the government.)

Government Exemptions and Surveillance Concerns

Moreover, the Act contains provisions that even explicitly exempt the government from anti-surveillance safeguards outlined in the law. Certain additional exceptions are created and applicable to 'regulatory or supervisory bodies', and crucial to the privacy rights landscape, there are no express standards for creating such exemptions. The lack of a provision related to foreign data processed in India, which the draft bill once had, may also have consequences for international cooperation and trust, notably when it comes to adequacy conclusions by supervisory authorities such as the European Union's.

Data Protection Board of India

The Act also calls for the establishment of a Data Protection Board of India (DPBI), which is charged with administering data-protection measures. But the Act limits the powers of the DPBI, which only functions in an adjudicatory capacity, meaning that it will lack the legislative powers to enable dynamic privacy law in response to technical change.

Concerns and Criticisms

It was roundly criticized because of questions concerning the potential for the Act to allow the government', and because the Act didn't explicitly provide for bodies to monitor what the government was doing in the name of data. The Act also earned criticism for having 'half-baked protections' and for affording the government overly broad exemptions that could result in wide swathes of specific privacy rights being pre-empted.

Impact on Businesses and Data Practices

For companies, the Act requires data processing agreements before data fiducia Tion outsourcing, and mandates financial consequences for non-compliance, including periodic Data Protection Impact Assessments for organisations that are 'significant' data fiduciaries. It fosters greater responsible data handling, and grants individuals' greater control over their data.

Landmark Judgments and Their Impact on Surveillance and Privacy

Through surveillance vs privacy debates, judicial interventions have carved out the space available for lawful state action as well as protected the integrity of individual rights. Judicial pronouncements on matters pertaining to privacy in India have truly influenced the nature of surveillance that is allowed, as well as determining what can be disallowed, and in what manner. Primarily among these is the judgment in K S Puttaswamy v. Union of India, which has been a game-changer in the Indian jurisprudence of privacy.

K.S. Puttaswamy v. Union of India

An unequivocal 9-judge bench judgment of the Supreme Court set out a different regime of legal interpretation about what is private, and exactly why it is so. Justice K S Puttaswamy (Retd) v. Union of India overruled previous judgments to the extent that they held that the Indian Constitution does not guarantee the right to privacy. The Court made a finding that the 'right to privacy is an intrinsic part of the right to life and personal liberty under Article 21 of the Constitution and other rights guaranteed by Part III of the Constitution.'

The Puttaswamy judgment established several critical principles:

- Privacy as a Fundamental Right: The judgment clearly ruled that privacy is a fundamental right, thereby ensuring that it receives the highest legal protection against arbitrary state action.
- Three-Part Test for Privacy Invasions: It established a three-part test for any government action seeking to breach fundamental rights of privacy: legality (a law exists); necessity (a legitimate state need); and proportionality (the least restrictive means to achieving the objective).
- Data Protection Principles: The Court also emphasized the importance of protecting your data. It suggested that the creation of robust laws to protect personal data from unlawful use are very important.

This judgment forms the foundation of assessments and guidance on surveillance, data protection and other related policies, laws and practices in India.

People's Union for Civil Liberties (PUCL) v. Union of India, in which the Supreme Court on the words of the Indian Telegraph Act, 1885, decided guidelines against arbitrary phone tapping. Its search for principles to separate arbitrary from routine surveillance, by strict adherence to laid-down procedures, specifically noted that wiretapping is an intrusion in a person's right to privacy, unless permitted under the procedure laid down by law. PUCL was the pathbreaking case to put in motion the detailing of privacy's extensions in Puttaswamy.

Justice K S Puttaswamy (Retd) v. Union of India (Aadhaar Judgment): In the aftermath of the landmark 2017 privacy judgment, the Supreme Court reviewed the constitutionality of the Aadhaar project. The court upheld the use of Aadhaar data for government welfare schemes and PAN linkage, but struck down large parts of the legislation that attempted to make Aadhaar mandatory for availing mobile connections and bank accounts, particularly because this was held to violate the right to privacy. The judgment reinforced the principle that, although the state can have a valid interest in collecting biometric data, such data-collection must be proportionate and not violate privacy rights in an arbitrary, disproportionate way.

Navtej Singh Johar v. Union of India: Though not specifically related to surveillance, the Navtej Singh Johar verdict, which struck down Section 377 that prohibited consensual sexual intercourse among adults of the

same sex, expanded the contours of the right to privacy. The Court held that privacy includes 'the right to be let alone', meaning that everyone has the right to keep all aspects of their private lives free from the intrusion of others, with a special emphasis on sexual intimacies. In other words, decisional privacy encompassed sexual autonomy, giving privacy a much broader scope under the Constitution.

These and other grounds have thus made for a complex cloth of case law that aims to both protect individual privacy on the one hand while, on the other, enabling state surveillance in certain and carefully defined circumstances. The jurisprudence that has been developed from them shows a sophisticated sensitivity towards the threats that technology poses to individual rights and freedoms, alongside the legitimate needs of the state.

Owing to the expansive scope of the judgments, whether in terms of issues addressed or the language of rights and entitlements, they will have a far-reaching impact on surveillance and privacy in the country. They have not only assured a constitutional space for privacy, but have also established the jurisprudential template for future legislation and policy on these issues.

Surveillance for National Security: Scope and Limitations

Surveillance takes a central position in the present system of national security in many countries, being employed to identify and intercept threats to the state or the people of the country (including citizens based in foreign countries), preventing or reducing those threats whenever possible. In India, national security entails the correction of many forms of institutionalized violence, and surveillance of various kinds, authorized by law in defense of the security of the state and individual rights, has emerged as one of the key strategies to ensure the country's security. The fact and manner of balancing the actual or perceived need for security and the accumulation and utilization of data to protect privacy rights calls for a close scrutiny of the legitimate (and illegitimate) uses of surveillance methods for the purposes of national security.

Legal Provisions Allowing Surveillance for National Security

- The IT Act, 2000: sections 69, 69A and 69B give the state the power to tap, intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource in the interest of sovereignty and integrity of India, the security of the state, friendly relations with foreign states, public order or for preventing incitement to the commission of any cognizable offence.
- •Indian Telegraph Act, 1885: Section 5 (2), where the central or state government is satisfied that it is necessary or expedient so to do, in the interests of the sovereignty and integrity of India, the security of the state, friendly relations with foreign states, public order or for preventing incitement to the commission of any cognizable offence, – intercept any message to or from any person or class of persons, or keep under surveillance the message to or from any particular person or class of persons; This Scheme merged into the Indian Telegraph Act of 1885, which led directly to the act's 2007 amendment, granting the state sweeping powers to intercept communications on grounds of national security – which the state planners have broadly construed to include anything that displeases them.
- The Unlawful Activities (Prevention) Act, 1967: An Act to provide for the prevention of certain unlawful activities association with the commission of which of the result of which involve

threat to the integrity of India, the security of the state, friendly relations with foreign states, or public order, or the commission of which are directed towards the overthrow of the government established by law in India by the use of force or other unlawful means;

These are legal authorities designed to allow the state to conduct surveillance for national security purposes, but they are also framed by standards of necessity, proportionality and review to ensure that they are not abused.

Case Studies: Implementation of Surveillance Measures in National Security Contexts

- Central Monitoring System (CMS): The CMS, or Centralized System for the interception of communications and related activities, is a system that allows authorities to intercept and monitor communications in accordance with the law. Despite the government's defense that the CMS is necessary to protect the state, leading to concerns that it could be misused as a surveillance tool against citizens and organisations without the proper checks and balances to protect them from abuse.
- Operation Blue Star (1984): Prior to Operation Blue Star, the state government had conducted extensive communications-interception operations and also collected intelligence on militant activity by the Khalistan. Though often regarded as necessary for the state's national security, the operation resulted in a substantial amount of pressure on civil liberties and the Sikh community.
- Kashmir and Counter-Terrorism: In conflict zones such as Jammu and Kashmir, surveillance plays a vital role in counter-terrorism operations. The use of drones, intercepts of signals and cyber-surveillance to trace movements of terrorists and to avoid casualties in terrorist attacks is testimony to the vital part played by surveillance. At the same time, civil liberties' concerns regarding electronic surveillance, the possibility of intrusion into privacy, the threat of abuse of personal rights etc call for strict checks and balances.

Critiques and Concerns Regarding Overreach and Abuse of Power

India's use of surveillance, although an important tool for national security objectives, has generated substantial criticism and concern regarding the potential for overreach and abuse of State power.

- No transparency or oversight: The existing legal framework is said to provide insufficient transparency or independent oversight, thus facilitating abuse of power; since we still have no stand-alone privacy law, and the safeguards contained in our existing laws are inadequate.
- Threat to privacy: Although projects such as the CMS and NATGRID have been designed for use in national security matters, there are great fears that they could be used for purposes of mass surveillance, involving the loss of privacy without either probable cause or judicial oversight.
- Disrespect for Civil Liberties: There are also cases of surveillance measures – particularly those implemented in sensitive areas or during times of civil unrest – perceived to constitute attacks on civil liberties, including freedom of speech and expression. The misuse of sedition laws, and new laws such as the Unlawful Activities Prevention Act (UAPA) in conjunction with surveillance data to

arrest human rights activists and dissenters, has been well-publicized.

- Judicial Interventions and the Shape of Reform: Finally, the judiciary, upon occasion, has been concerned to regulate surveillance and privacy. While the Supreme Court in K S Puttaswamy has asserted the nature and value of privacy, and formulated some principles that could delineate the boundaries and parameters of surveillance and data collection beyond arbitrary state action, such judgments indicate the role of the judiciary in surveillance in a democracy.

In India, the discourse on national security surveillance is a balancing act between legal mandates, national imperatives and human rights, with the state's interest in protecting its citizens being beyond reproach, yet its machinations being tempered by the court-imposed threshold of legality, necessity and proportionality to prevent the derogation of democratic freedoms and individual liberties. Given the nature of evolving threats and technology, there is a need for deliberation, judicial scrutiny and legislative reform to evolve a nuanced approach whereby the imperatives of national security strike a balance vis-à-vis privacy rights.

The Debate: National Security vs. Individual Privacy

Realizing that authoritarian control over our private life's rests on a bedrock of knowledge About whether individual privacy rights or collective national security should be the top concern remains one of the biggest dilemmas of democracies across the world. For some, any increase in surveillance is necessary for national security, battling terrorism, cybercrime, foreign threats, etc. While others believe that privacy rights of individuals are crucial for keeping democracy strong, protecting citizens from misuse of power, and ensuring the right of free speech. This is a discursive fight that is a multilayered, complex and absolutely nuanced argument. It can be seen as an ideological response to the fact that our discourse is changing with the increasing pace of going digital on a global scale.

Arguments for Enhanced Surveillance for National Security

- Terrorism threats: India's geo-political situation and history of terror — both internal and cross-(border) terrorism — demands that a surveillance net be strong. Proponents of surveillance say it helps thwart terror plans, track terrorist movements, and break up networks that threaten the country's unity and integrity, and the safety of its residents. Numerous scholars have separately tried to measure the 'magnitude of imperfections' that states with significant internal threats have incentive to invest in monitoring citizens, independent of wealth. (Peak-welfare states do not surveil their citizens, since they have no reason to doubt their loyalty.) The Muslim majority state of Jammu and Kashmir has come under increased scrutiny because of its location in regions prone to terror.
- Cybercrime: Due to the digital revolution, cybercrime has become the most menacing challenge for the national security, the economy and the private lives of the citizens. Surveillance including the cyber spaces and digital transactions became the only way of detecting and punishing those cybercrimes such as the hacking, impersonation, savings theft etc, in addition to it, whatever new appears in the digital infrastructure it welcomes the surveillance
- External Aggression: Beyond traditional spying, this includes satellite images, cyber espionage and signals intelligence. It is seen here as defensive, in order to make quick, informed decisions about territorial integrity and national sovereignty.

Arguments for Prioritizing Individual Privacy Rights

- Misuse: Critics of mass surveillance have warned about the risk of misuse and abuse of power. Without strong safeguards, they warn, the requesting state might use the data collected for its own political repression of dissidents, among other rights-fixing violations.
- Impact on democracy: An open, accountable and rights-respecting democracy flourishes through openness, accountability and respect for the freedoms of citizens. Mass surveillance without commensurate and strong legal protections is not only beyond democracy but also corrosive to debate and dissent, and violent to the free movement of ideas. The chilling effects on free speech – where people do not say things in case they are being watched – is itself a direct attack on the life of democracy.
- Chilling effect on free speech: The chilling effect on free speech can be consequential. People might self-censor speech or behaviour (marching, teaching, lecturing, posting in social media) to avoid government scrutiny. Aside from being an affront to democracy, such an outcome will stunt innovation, creativity and social progress.

Balancing Act

There are no easy solutions; nor do the issues lend themselves to binary thinking. Rather, the balance requires us to constantly engage with the interplay of changing threats, technologies, their applications – and, most important, the imperatives of a democratic society grounded in privacy and a belief in the freedoms that underpin it. Beginning with K.S. Puttaswamy v. Union of India, through which it set down the law defining privacy as a fundamental right with reasonable restrictions that the state can place in the name of national security, the judiciary has now laid some tentative ground rules to govern the balancing act.

The debate on national security versus the rights of an individual to privacy in India is part of the larger global debate on how to balance a digital present burdened with ubiquitous data and omnipresent surveillance technologies. It is also an elaboration of how national security can be ensured without curtailing the democratic freedoms and the right to privacy that underpin a free society. The debate continues, and will continue to set the contours of law, policy and values in India in the years to come, provided that it is monitored judiciously, fences are mended with robust legal structures, and the citizenry is informed enough to see through the tropes.

International Comparisons

As such, the ongoing social and political conflict over surveillance versus privacy is not unique to India. It is a focal point of debate across democracies in the world with each nation formulating and implementing its own version of this story shaped, initially, by past historical, cultural and legal contexts supporting its deliberations. The US, the UK and the EU provide a foundational framework for understanding the variety in approaches deployed to arrive at a balance between national security interests and the protection of individual privacy rights. Together, they reveal the international dimensions to this challenge, as well as functioning as a storehouse of lessons and best practices germane to India's ongoing engagement with these issues.

Surveillance and Privacy in Other Democracies

United States (USA): Thanks largely to the Parallel Construction rule, the USA's surveillance apparatus – and the US National Security Agency (NSA) in particular – has been among the most powerful in the world since 9/11. This power was explicitly granted to US intelligence agencies via relevant legislation such as the Patriot Act and the subsequent implementation of the Foreign Intelligence Surveillance Act (FISA) that authorized mass surveillance measures. Edward Snowden's revelations in 2013 (and the subsequent national and global public debate about the balance between security and privacy) culminated in further attempts to regulate domestic surveillance. This included the USA Freedom Act of 2015, which placed restrictions on the collection of telecommunication metadata.

United Kingdom (UK): One of the most expansive surveillance regimes in a democratic country is the Investigatory Powers Act 2016, popularly known as the 'Snoopers' Charter', with huge and invasive powers to snoop on and track Internet browsing histories, hack into personal devices and metadata, and to make bulk data collection for analysis. While these powers have been sold to the public as safeguarding national security, there have been significant concerns raised about the regulation of privacy and freedom of speech. As a response, the UK has put in place surveillance oversight systems, such as the Investigatory Powers Commissioner's Office (IPCO) to even check whether surveillance efforts are proportionate and moderate.

The European Union (EU): The EU, by contrast, is a 'privacy'-focused model, which explicitly recognizes the protection of personal data and privacy as fundamental rights under the Charter of Fundamental Rights of the European Union. From 2018 onwards, with the entry into force of the General Data Protection Regulation (GDPR), all those living in the EU and the European Economic Area must comply with some of the strictest rules of data protection and privacy for both private and public actors. The EU model recognizes that, especially online, surveillance and violation of privacy are inevitable and have become deeply intertwined with the daily practices of Big Data companies, states and many other forms of governance. The GDPR's approach to privacy and data protection has become a global benchmark, emphasizing the need to have as little data as possible on people and as many consumers as possible to maintain a free and democratic society, and often to enable democratic engagement with businesses, states and others. The EU demands maximum levels of transparency and accountability from both private and public actors.

Mitigation Strategies and Suggestions

This complex interplay between the need for public surveillance for national security and the equal need to safeguard the honored rights of individuals requires a balanced approach. Minimizing the risk of conflict between the twin objectives of security and safeguarding of individual rights requires legal reform, technological innovation and effective checks and balances.

Legal Reforms for Enhancing Privacy Protections

A necessary step towards mandating globalized privacy standards is the amendment in laws that are outdated in relation to modern-day privacy standards and technologies. For e.g., the Indian Telegraph Act, 1885 and the Information Technology Act, 2000 can be recalibrated to include express privacy safeguards that enumerate clear, narrow intelligible bases under which the privacy of any individual can be breached. The

amendments must be confined to procedural safeguards by making judicial warrants a mandatory for the conduct of surveillance, thereby also precluding arbitrary and indiscriminate collection of data.

New legislation should be introduced and it should include a robust and comprehensive data protection law, modelled on something like the European Union's General Data Protection Regulation (GDPR), spelling out individuals' rights with respect to their personal data, what constitutes consent, the states' obligations for the protection of data, and severe penalties for violation. The law should also deal with the distinct challenges presented by state surveillance by attempting to find a realistic balance between necessary state surveillance for matters of national security, and the individual right to privacy.

Technological Solutions to Safeguard Privacy Without Compromising Security

End-to-end encryption of communications and anonymization of data to prevent identification of individuals might be used where privacy could otherwise not be adequately protected. Hence, the right to privacy will not be blurred with data security demands of the smart state. These technologies would help to protect privacy without preventing state agencies from achieving the legitimate objectives of their surveillance programmes. They would secure data so that it would be unintelligible to others while still permitting lawfully authorized interception of the communication by security agencies.

Collecting data requires a robust data storage solution with strict data access controls used. You can add extra layers of security when sharing user information by using a biometric lock to access the data, or integrating the collected data in a blockchain data storage system to make it tamper-proof and only visible to genuine owners.

Oversight Mechanisms: Judicial Review, Parliamentary Oversight, and Independent Bodies

Give the judiciary more 'bite' as a day-to-day supervisor of intelligence and surveillance activities This might even involve the establishment or strengthening of a formal, independent judicial body or tribunal to approve and/or grant warrants for surveillance applications. This would ensure that the individual's privacy is appropriately balanced and in accordance with the rule of law.

Mandatory reporting to Parliament of the powers exercised at intervals, together with Parliamentary debate and scrutiny and oversight, could help to maintain a level of parliamentary accountability and scrutiny, as well as fostering the principle of surveillance being transparent, accountable and responsive to democratic scrutiny. This would in turn have the effect of holding Parliament to account in the eyes of the public – to ensure that it fulfils its duty of ascribing accountability for the operations of surveillance powers and whether the Intelligence Services were exercising powers during times of crisis in a manner proportionate to the threat and also not disproportionately affecting human rights. Parliaments have an opportunity to step up to the plate and begin to draw a positive picture of the role their members can play in maintaining transparent, accountable and democratic surveillance operations. Meanwhile, the Surveillance Commissioner in the UK has internationally recognized expertise in surveillance, holds national security information, and has continually shown expertise in this field.

Complaint-investigating oversight bodies, surveillance auditing and reporting bodies, and those that make recommendations for reform, could be challenged and modulated by an additional level of control if they

could subpoena all relevant information and had the necessary expertise to make independent assessments of the lawfulness and necessity of any given surveillance operation.

Future Outlook

As for whether India finds itself in this awkward position about the future of surveillance and the future of privacy in general, the answer is: yes and no. First, it is yes because what caused a glitch in terms of the enforcement of the lockdown was our failure to fully account for an accelerated technological landscape as well as an equally quickened social terrain. The intrusion by AI and facial-recognition technologies into human affairs post-curfew is an artificial intelligence and facial-recognition pre-lockdown word. What India is facing now is post-curfew, post-lockdown. The lie was that surveillance offered India a qualitatively different kind of national security but no, because today, these technologies have reified the possibilities of what was already an exceptional structural prerequisite for a large-scale erosion in individual privacy. It is no longer a question of whether India will find this impossible needle to thread these diffuse interests and make legal, technical and oversight systems that protect rights, or, whether we will falter and allow AI to undo the privacy of a vast number of Indians. It is also no longer a question of when India will catch up with technology, only that we will.

Emerging Technologies and the Future of Surveillance

- AI: One of the great strengths of artificial intelligence would be its ability to analyses very large data sets; this could be used to mitigate threats to national security from identifying patterns that predict terrorism to blocking the first stages of possible cyber-attacks. But AI-based surveillance would also raise important issues for privacy, discrimination, and accountability, particularly if algorithms make determinations about rights without clear or discernible criteria.
- Facial Recognition: Use of facial recognition software is on the increase in law enforcement and security agencies worldwide, such as in India. This technology can assist greatly in identifying criminals and potentially preventing crimes before they occur. However, it remains quite controversial from a privacy perspective. The questions surrounding the possibility of mass surveillance, erroneous identification of people, and loss of anonymity in public spaces need to be addressed.
- Internet of Things (IoT): the proliferation of IoT devices augments the capabilities of surveillance into the inner-most spaces of peoples' lives, collecting data that can be immensely revealing, and thereby requiring the highest possible protections against abuse and leaks.

Evolving Challenges to Privacy in the Digital Age

The challenges brought by the so-called 'digital age' exacerbate the problem. The huge quantities of data collected and processed by private entities and the state, the black-box quality of algorithmic decisions, and the fact that these activities span the globe in terms of both participant and audience mean that the protection of privacy depends on the cooperation of many more than just the individuals whose privacy is at issue.

A second major risk is the danger of function creep: using data for a purpose different from the one for which it was originally collected. This danger is heightened in the world of new technologies that can track and analyses data instantly – and often without our knowledge and consent.

Prospects for a Balanced Approach in India

If India is to succeed in negotiating the new terrain of surveillance and privacy, it should adopt a multilayered approach combining legal reforms, technological safeguards and innovative oversight mechanisms.

It is crucial to have regulations in place to keep pace with technological advancements, such as laying out explicit prohibitions on certain state uses of AI and facial recognition, overhauling data protections, and creating greater visibility and accountability around the use of surveillance.

Generous government funding of technologies that improve personal privacy – for example, generalized anonymization technologies, encryption tools, generalized 'privacy by design' tools – can greatly lessen these risks.

Enhance the accountability measures on surveillance powers, whether through judicial, parliamentary or independent regulatory oversight, to ensure that such powers are limited to that which is necessary for attainment of the purpose associated with the law, and that there is no unreasonable or unlawful invasion of the privacy of the individual.

Participating in international forums to exchange knowledge, develop shared norms and standards, and co-ordinate cross-border data-protection and surveillance oversight can help enhance international privacy and surveillance regulation.

Conclusion

It is a complex story of the interplay between national security and the rights of the individual by dint of historical developments, legal regimes and critical judicial pronouncements. India's national security architecture is deeply invested in surveillance regimes that leverage the persuasive power of technologies that include Aadhaar, CMS, NETRA and NATGRID that serve the purposes of the state in grappling with national, human and cyber security threats. At the same time, the very same technologies are beset with serious privacy concerns. Such concerns have found their judicial resolution, the latest being K S Puttaswamy (Retd) v. Union of India where the Supreme Court has declared privacy as a 'constitutional' right, fettering state action that impinges upon an individual's right to privacy to lawfulness, necessity and proportionality.

Meanwhile, the regulatory framework – provisions under the IT Act 2000, the Indian Telegraph Act 1885 and draft legislations such as the Digital Personal Data Protection Act 2023 – illustrate how the highly specialized discipline of constitutional rights jurisprudence and emerging privacy frameworks in India try to operationalize the constitutional history of surveillance. These measures have critiques themselves for being overreaching, and require improved and robust mechanisms of oversight, transparent governance and accountability to prevent abuse, violation and misuse, and ensure greater necessity and proportionality in surveillance.

After all, it is judge's ruling in cases of fundamental importance who can ultimately impose the limit on state surveillance, and who can underline the vital role of privacy rights in sustaining democratic life. The flow of ideas demonstrates the continued necessity for legal reform, technological invention, and independent oversight of state surveillance to protect human freedoms. This balance preserves both public trust in public institutions as well as the fabric of democracy and the rule of law.

Ultimately, therefore, the direction of India's surveillance and privacy tomorrow, and particularly in a scenario of rapid technological change, smart cities, strong security needs and fast digital transformation, lies in the fine line of balancing collective security requirements in the name of India's often loudly proclaimed democratic peace with respecting human rights and guarding against abuse. Legal reform, technological controls and better oversight mechanisms will be the way forward. As India evolves in this regard, democracy, the rule of law and due regard for individual rights are at the heart of the global competition in the surveillance and privacy arena.

REFERENCES

1. Ahmad, N. (2009). Restrictions on cryptography in India – A case study of encryption and privacy. *Computer Law & Security Review*, 25(2), 173-180. https://doi.org/10.1016/j.clsr.2009.02.001
2. Balancing right of privacy and national security in the digital age. (2017, September 24). Retrieved from https://capsindia.org/wp-content/uploads/2021/10/CAPS_ExpertView_AKG_01.pdf
3. Bhandari, V., & Lahiri, K. (2020). The surveillance state: Privacy and criminal investigation in India: Possible futures in a post-Puttaswamy world. *Univ. of Oxford Human Rights Hub Journal*, 3(2), 15. Retrieved from https://ssrn.com/abstract=3580630
4. Bhatia, G. (2014). State surveillance and the right to privacy in India: A constitutional biography. *National Law School of India Review*, 26(2), 127–158. Retrieved from http://www.jstor.org/stable/44283638
5. Chadha, V. (2022). Balancing the privacy v. surveillance argument: A perspective from the United Kingdom. Retrieved from https://repositorio.ual.pt/bitstream/11144/5433/1/00EN-vol13-n1-art012.pdf
6. Chadha, V., Coimbatore Balasubramanian, T., & Bhuwalka, A. (2022). Privacy and surveillance conflict: A comparative analysis of the laws in the USA and India. Vol. 13, No. 2 (November 2022-April 2023), 201. Retrieved from https://repositorio.ual.pt/bitstream/11144/5668/1/11-EN-vol13-n2-art08.pdf
7. Chandak, L. (2017). Privacy and Data Security – a National Need. Retrieved from https://trai.gov.in/sites/default/files/Span_Technology_07_11_2017.pdf
8. Dembi, D. (2021, January 30). Privacy & National Security: A Balancing Act? *SSRN*. https://dx.doi.org/10.2139/ssrn.3953357
9. Digital rights vs. national security: Balancing privacy and surveillance in the era of mass surveillance and cyber threats. (2023, July 18). Retrieved from https://juriscentre.com/2023/07/18/digital-rights-vs-national-security-balancing-privacy-and-surveillance-in-the-era-of-mass-surveillance-and-cyber-threats/
10. Fontes, C., Hohma, E., Corrigan, C.C., & Lütge, C. (2022). AI-powered public surveillance systems: why we (might) need them and how we want them. *Technology in Society*, 71, 102137. https://doi.org/10.1016/j.techsoc.2022.102137
11. Fox, G., Clohessy, T., van der Werff, L., Rosati, P., & Lynn, T. (2021). Exploring the competing influences of privacy concerns and positive beliefs on citizen acceptance of contact tracing

mobile applications. *Computers in Human Behavior*, 121, 106806. https://doi.org/10.1016/j.chb.2021.106806

12. Greenleaf, G. (2010). India's national ID system: Danger grows in a privacy vacuum. *Computer Law & Security Review*, 26(5), 479-491. https://doi.org/10.1016/j.clsr.2010.07.009

13. Gupta, A., & Bhandari, V. (2021, December 20). National security, at the cost of citizens' privacy. *The Indian Express*. Retrieved from https://indianexpress.com/article/opinion/columns/national-security-at-the-cost-of-citizens-privacy-7680787/

14. Gupta, S., & Negi, S. (2024, February 10). Detangling the knots: Privacy vis-à-vis surveillance. Retrieved from https://sclhrblogs.in/2024/02/10/detangling-the-knots-privacy-vis-a-vis-surveillance/

15. Harkauli, A. (2023, August 3). The fine balance — Surveillance, security, and the right to privacy. Retrieved from https://www.scconline.com/blog/post/2023/08/03/the-fine-balance-surveillance-security-and-the-right-to-privacy/

16. Javvaji, S. (2023, July). Surveillance Technology: Balancing Security and Privacy in the Digital Age. *EPRA International Journal of Multidisciplinary Research (IJMR)*, 9(7). https://doi.org/10.36713/epra13852

17. Justice K.S. Puttaswamy & Anr. vs. Union of India. *Writ Petition (Civil) No 494 of 2012; (2017) 10 SCC 1; AIR 2017 SC 4161*. Supreme Court of India. Decided August 24, 2017.

18. Kaur, R. (2018). Surveillance and Privacy: A Ramification of Article 21. *International Journal of Reviews and Research in Social Sciences*, 6(3), 284-290.

19. Kumar, C. (2023, October 4). Government surveillance and the erosion of the right to privacy. Retrieved from https://www.linkedin.com/pulse/government-surveillance-erosion-right-privacy-chetan-kumar/

20. Lane Fox, M., & Cross, T. (2015). Is privacy more vital than national security? Index on Censorship, 44(1), 112-116. https://doi.org/10.1177/0306422015571513

21. Moyakine, E., & Tabachnik, A. (2021). Struggling to strike the right balance between interests at stake: The 'Yarovaya', 'Fake news' and 'Disrespect' laws as examples of ill-conceived legislation in the age of modern technology. *Computer Law & Security Review*, 40, 105512. https://doi.org/10.1016/j.clsr.2020.105512

22. Nam, T. (2019). What determines the acceptance of government surveillance? *The Social Science Journal*, 56(4), 530-544. https://doi.org/10.1016/j.soscij.2018.10.001

23. Nandy, D. (2023). Human rights in the era of surveillance: Balancing security and privacy concerns. *Journal of Current Social and Political Issues*, 1(1). https://doi.org/10.15575/jcspi.v1i1.442

24. Navtej Singh Johar vs Union of India Ministry of Law. *AIR 2018 SC 4321*. Supreme Court of India. Decided September 6, 2018.

25. Pegasus in the room: Law of surveillance and national security's alibi. (2021, August 7). Retrieved from https://www.orfonline.org/expert-speak/pegasus-in-the-room-law-of-surveillance-and-national-securitys-alibi/

26. People'S Union of Civil Liberties vs Union of India (UOI). *AIR 1997 SC 568.* Supreme Court of India. Decided December 18, 1996.

27. Privacy in the Digital Age: Legal Aspects and Protection in India. (2023, August 10). Retrieved from https://www.legalmantra.net/blog-detail/PRIVACY-IN-THE-DIGITAL-AGE-LEGAL-ASPECTS-AND-PROTECTION-IN-INDIA

28. Rana, S. (2023, August 19). Privacy Rights and Surveillance in the Digital Media Space: Constitutional Concerns, Challenges and Need for Reforms in India. Retrieved from https://sclhrblogs.in/2023/08/19/privacy-rights-and-surveillance-in-the-digital-media-space-constitutional-concerns-challenges-and-need-for-reforms-in-india/

29. Rizvi, K. (2019, December 17). Why Privacy And Security Should Go Hand-In-Hand: The Balancing Act. Retrieved from https://inc42.com/resources/why-privacy-and-security-should-go-hand-in-hand-the-balancing-act/

30. Rizvi, K. (2020, July 11). Personal data protection bill 2019 and surveillance: Balancing security and privacy. Retrieved from https://inc42.com/resources/personal-data-protection-bill-2019-and-surveillance-balancing-security-and-privacy/

31. Saglam, R.B., Nurse, J.R.C., & Hodges, D. (2022). Personal information: Perceptions, types and evolution. *Journal of Information Security and Applications*, 66, 103163. https://doi.org/10.1016/j.jisa.2022.103163

32. Saura, J.R., Ribeiro-Soriano, D., & Palacios-Marqués, D. (2022). Assessing behavioral data science privacy issues in government artificial intelligence deployment. *Government Information Quarterly*, 39(4), 101679. https://doi.org/10.1016/j.giq.2022.101679

33. Shekar, K. (2022, February 17). The state of surveillance in India: National security at the cost of privacy? Retrieved from https://www.orfonline.org/expert-speak/the-state-of-surveillance-in-india

34. Striking a Balance between Privacy, Security. Retrieved from https://www.thehindubusinessline.com/business-laws/striking-a-balance-between-privacy-security/article34806162.ece

35. Tiwari, A. G. (2024, February 4). Administration of the nexus: National security vs. privacy in government surveillance programmes. Retrieved from https://primelegal.in/2024/02/04/administration-of-the-nexus-national-security-vs-privacy-in-government-surveillance-programmes/

36. Van Daalen, O.L. (2023). The right to encryption: Privacy as preventing unlawful access. *Computer Law & Security Review*, 49, 105804. https://doi.org/10.1016/j.clsr.2023.105804

37. Yadav, A. (n.d.). The real struggle for privacy and national security in terms of liberty and surveillance. Retrieved from https://theamikusqriae.com/the-real-struggle-for-privacy-and-national-security-in-terms-of-liberty-and-surveillance/