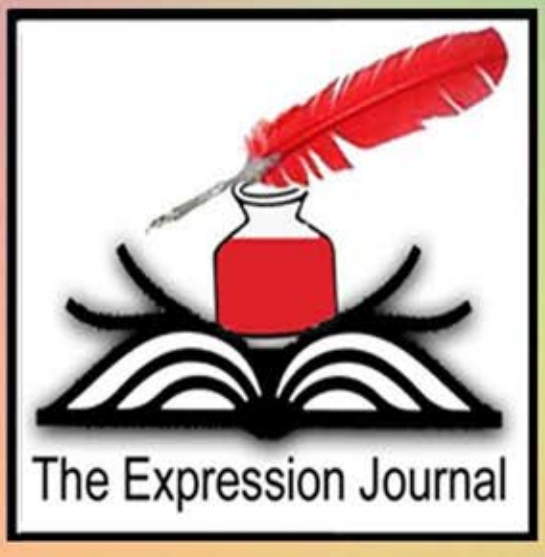
ISSN : 2395-4132

THE EXPRESSION

An International Multidisciplinary e-Journal

Bimonthly Refereed & Indexed Open Access e-Journal



Impact Factor 6.4

Vol. 11 Issue 5 October 2025

Editor-in-Chief : Dr. Bijender Singh

Email : editor@expressionjournal.com

www.expressionjournal.com

The Expression: An International Multidisciplinary e-Journal
(A Peer Reviewed and Indexed Journal with Impact Factor 6.4)
www.expressionjournal.com ISSN: 2395-4132

State Surveillance vs. Privacy Rights: A Critical Analysis of Aadhaar, Pegasus, and Other Digital Privacy Concerns

Mr. Anurag Suthar
Research Scholar
Faculty of Law, Tantia University, Sri Ganganagar
Dr. Atul Kumar Sahuwala
Research Supervisor
Faculty of Law, Tantia University, Sri Ganganagar

Abstract

The rapidly developing digital technologies not only changed the provisions of governance, security, and citizen-involvement, but they have managed to raise a question of whether the state should be given a license to snoop on their own citizens and invade their privacy or not. Such tension is best noted in scandals on the Aadhaar scheme, and the Pegasus spyware leak and other emerging trends of digital surveillance in India. Although people on the right defend the surveillance activities claiming that the national security, welfare provision and even control of the crime, the dissenters take caution that too much power of a state over the internet is expected going to diminish the constitutional freedoms and even the democratic accountability. This issue is critically examined in this paper concerning legal, ethical, and policy facets, that are of high-profile cases that have brought not only questions to the psyche of people but also to the justice system in India. It is founded upon the constitutional, judicial and international perspectives and investigates the adequacy of the existing security against the attacks on privacy and concludes about the weaknesses in the mechanism of examination and responsibility. Through a convergence of a set of doctrinal legal analysis and policy analysis, the paper sheds otherwise needed and rights-appropriate light on a proportionate and democratic-minded yet technologically nimble measure-of policing that should be instituted. The findings emphasise that, in the case that effective legislative frameworks are not in place, independent supervisory controls and the enhanced recognition of the masses, there is the long-term risk of the threat of normalisation of intrusive surveillance compromising the civil liberties.

Keywords

Aadhaar, Pegasus, Digital Privacy, Surveillance Law, Right to Privacy, AFRS, Data Protection Act 2023, Judicial Oversight, Independent Regulator, Civil Liberties.

The Expression: An International Multidisciplinary e-Journal
(A Peer Reviewed and Indexed Journal with Impact Factor 6.4)
www.expressionjournal.com ISSN: 2395-4132

State Surveillance vs. Privacy Rights: A Critical Analysis of Aadhaar, Pegasus, and Other Digital Privacy Concerns

Mr. Anurag Suthar
Research Scholar
Faculty of Law, Tantia University, Sri Ganganagar
Dr. Atul Kumar Sahuwala
Research Supervisor
Faculty of Law, Tantia University, Sri Ganganagar

Introduction

The digitalization of government has not only rendered state business more efficient, fast and accessible than ever but has also been changing the connection between the state and the individual in a way that can only call the traditional understanding of privacy and liberty into question. The interactions among colossal regimes of identity, sophisticated apparatus of surveillance and data-based methods of governance in India has rendered the debates over the accommodable realms of state power in the virtual space more disputable. Justice, K.S. Puttaswamy v. the constitutional expression of right to privacy.[1] The case of Union of India was also a milestone of the Indian jurisprudence but the reality of operation of this right in these current developments of surveillance remains doubtful.

Central here is the Aadhaar programme, a biometric-authentication unique identification scheme firstly proposed on top of the voluntary restructuring of welfare methodology that has gradually turned into near-constitutional hostility just before access to a geographically broad range of services. Though the supporters express it in a very positive tuna, its intendment to reduce fraud or be efficient, its opponents point out the state profiling, surveillance and exclusion thus creating massive concern on privacy matters.[2] Similarly, it was proven by the Pegasus spyware scandal that even more sophisticated digital surveillance tools will apparently be employed to ask journalists, activists, and political leaders on the basis that their use is both reasonable security steps and suppression of dissent.

Such tendencies are part of a bigger trend in the globe that goes towards technical capacity on the state in areas like policing and the managing of the boundaries as well as the well being of the individual and administration of finance. Such changes

[1] *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) 10 SCC 1.
[2] Baxi, Upendra, *The Future of Human Rights* (New Delhi: Oxford University Press, 2012) p. 144.

necessitate a highly significant study of the lawfulness and institutional provisions which are expected to check against the intrusion of the citizens in an undue and arbitrary manner. Although the most recent government measures, including the Digital Personal Data Protection Act, 2023, can be discussed as signifying a grasp of these problems, the question arises as to whether control, transparency, and accountability are active enough or not.[3]

This debate is further increased by the global context. Balancing between privacy entitlement and national security needs has proven to be challenging and has allowed some jurisdictions, including the European Union, the United States of America and the United Kingdom, to showcase success stories and lessons. It is within this broader context that this paper places the India experience in an attempt to bring to an informed debate on the future of privacy and surveillance in democratic societies.

Objectives of the Study

1. To critically examine the constitutional, legal, and ethical dimensions of state surveillance in India.
2. To analyse the privacy implications of Aadhaar, Pegasus, and other digital surveillance mechanisms.
3. To assess judicial and legislative responses to digital privacy concerns in India.
4. To compare India's surveillance and privacy framework with selected international models.
5. To propose policy recommendations that balance privacy rights with legitimate state interests.

Research Methodology

This study adopts a **qualitative, doctrinal research approach**, relying primarily on secondary data sources. It draws upon constitutional provisions, statutory frameworks, judicial decisions, parliamentary reports, and policy documents to analyse the legal dimensions of privacy and surveillance. Case study analysis is applied to examine the Aadhaar programme, the Pegasus spyware controversy, and other notable instances of digital monitoring. Comparative perspectives are incorporated through a review of international legal frameworks and scholarly literature from jurisdictions with established privacy safeguards. Academic articles, think tank studies, and investigative journalism form the basis for contextual and critical evaluation. The research employs a normative lens, using constitutional values and human rights principles as benchmarks to assess the proportionality, necessity, and legality of surveillance measures.

Privacy Rights and State Surveillance in India

The recognition of privacy as a fundamental right in India has evolved gradually, shaped by judicial interpretation rather than explicit constitutional text. While the Constitution of India does not expressly mention the right to privacy, the Supreme Court in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) affirmed it as intrinsic to the right to life and personal liberty under Article 21.[4] This landmark nine-judge bench decision established privacy as a multi-dimensional right encompassing personal autonomy, informational control, and decisional freedom. The case highlighted that any

[3] Schwartz, Paul M., "Internet Privacy and the State" (2000) 32 *Connecticut Law Review* 815.
[4] *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) 10 SCC 1.

violation of privacy by the state has to meet the legality, necessity and proportionality test and this puts privacy within the constitutional administration of affairs.

But this expansion of state capacity to monitor the activities of its citizenry has ever been seen in this time. The development of digital technologies, such as biometric authentication, facial detection, data mining, and tracking solutions based on artificial intelligence, allowed the state to gather, retain, and process personal information in an order of magnitude that has never been seen before. Although these capabilities can be useful in crime prevention, counter-terrorism and effective provision of government services, they also increase the risk of abuse and mission creep where equipment developed to solve one mission is steadily expanded to the other without much oversight. In India, no general surveillance law exists so most of this activity falls within the provisions of isolated reading in the Telegraph Act, 1885, the Information Technology act, 2000, and other relevant rules, which have a weak procedural guarantee according to critics.[5]

The Aadhaar ecosystem captures the future of government power and the future of an oppressive governance. The system has resulted in a consolidated information storage of the citizens after connecting the distinctive biometric identifiers to income maintenance, the welfare remittances as well as cellular relationships. Even as the constitutionality of this scheme on welfare grounds was affirmed by the Supreme Court in its 2018 Aadhaar practice, clauses requiring the use of this specific scheme to access privately provided services were also invalidated, which suggests that judges are uncomfortable with data collection without restrictions. However, the amendments that have been introduced after, have somewhat erased these restrictions, raising the question of the effectiveness of privacy protection.

Alongside Aadhaar, the Pegasus spyware being publicized in 2021 demonstrated the feasibility of having the targeted highly intrusive surveillance being employed without receiving any legal sanction.[6] The complexity of Pegasus in its capacity to compel feasibly all data out of the device to which it directs its extraction presents difficulties to both the historian Protestantism's such as the unjustifiable warrants being served in court or its process. The lack of covering facts on the case, even though the same was commissioned to an independent committee by the Supreme Court, has left many gaps especially on the accountability and the corrective actions to the involved citizens.

The privacy scenario of India, being more general, is also not that simple since the government interacts with the non-governmental sides of the regulation of the data collection process. It is also common to find telecommunication organizations, internet providers, and social media services as the element in between, through which the kind of state surveillance is exercised with either the assistance of legislation enforcement or in an informal sense. The Digital Personal Data Protection Act, 2023 is also the remarkable law regarding the consumer protection of the data, yet the consent of the governments on the exemptions and low due to disclose the members of the privacy community came under criticism.

[5] David Lyon, *Surveillance Studies: An Overview* (Cambridge: Polity Press, 2007) 66.
[6] *Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act* 2016.

Case Studies – Aadhaar, Pegasus, and Other Digital Privacy Issues

The contextual shift of digital governance in India has led to the vary of surveillance practices that are considered measures of efficiency, and others refer to it as a security measure. It will be possible to see closer at some case studies that will provide a better prism to understand the relationship between technology, the law, and civil liberties. The most high-profiled of them were the scandal of Aadhaar identity and the Pegasus spyware scandals and other recent scandals, such as the mass facial recognition programs and surveillance settings on social media. Collectively, they depict the multiplicity of surveillance instruments and the frequently repeated inadequacy of control, permissible lack of clarity of law, and legal controversy.

The Aadhaar system can be seen as the most extensive data infrastructure that has been implemented in India. Started as a voluntary biometric identity program aimed at attacking the targeted referral administration of welfare services, it soon spread to become nearly a universal condition of accessibility to any governmental service, and at one point period, even to site access to any non-government fringe such as banking and telecommunication services. Although the Aadhaar was by the government presented as a failure over in order to combat duplication and fraud, there were criticisms of a centralised repository of a sensitive biometric information, lack of a solid opt out option as well as the possibility of profiling.[7] Its constitutional validity was affirmed but limited to allow others to use it as a matter of necessity to the work of a private sector in its activities and functions, the judgment of the Supreme Court of 2018 made - it was later softened in part due to legislative changes.

In 2021, the Pegasus spyware scandals put the issue of such targeted surveillance into the limelight. Pegasus is a product of the NSO Group that can easily penetrate the devices, without the user involvement and scans messages, call history, encrypted chat, and even remotely uses cameras and microphones.[8] Claims that it was employed against journalists, activists and political opponents elicited intense public and legal investigations. When the Supreme Court ruled to have an independent expert committee, it was an indicator that the matter is not something light but the full disclosure of the findings remains hidden has thrown the trust of the people into a narrow path.

Also, besides these high-profile cases, there is the Automated Facial Recognition System (AFRS) plus internet shut down ordinances habitually installing features of monitoring much like the Automated Facial Recognition system, and even the explanation of mechanisms to spy on their activities so that the system of law enforcement might keep an eye on them. The two of them raise questions about the proportionality, openness, and the inexistence of particular statutory restrictions of their boundaries and terms.[9]

Legal, Judicial, and Policy Responses

The connectivity in the direction of India that defines and protects the right to digital privacy has been identified by effects of various watershed judicial determinations, legislation and even policy activities. Nevertheless, this process has not

[7] Jain, Shruti, "Aadhaar and the Right to Privacy" (2019) 4 *NALSAR Student Law Review* 201.
[8] Greenleaf, Graham, "Pegasus and the Global Spyware Problem" (2021) 171 *Privacy Laws & Business International Report* 12.
[9] Agrawal, Ritu, "Biometric Surveillance and Civil Liberties" (2020) 55 *Economic and Political Weekly* 47.

been linear, but it has depicted the active tensions between the growing state authority to monitor the populace and minority constitutional rights of personal freedom. Lack of specific legislation on surveillance also implies that laws better ensure protection, even though judicial measures frequently rely or sectoral regulations which are haphazard.
The courts have had an active role in formulating the discourse. Earlier examples, e.g., of Kharak Singh v. The case of State of Uttar Pradesh (1963) recognized the elements of privacy indirectly. Union of India (2017) that declared privacy rights category. In this decision, the proportionality test of state intrusions was born and preceding states basic legality, necessity, and proportionality were established as necessary conditions of legal restrictions.[10]

At the legislative level, biometric identity programme was formalised by the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, though its scope and a compulsory character were challenged several times in the courts. In 2018 Puttaswamy (Aadhaar). Where the Supreme Court supported the welfare-focused use of the scheme but limited its extension into the private sector. These restrictions were watered down later, and that captures the phenomenon of progress and retrogress beside the policy considerations called privacy protection.[11]
In 2021, the judiciary involved in the case because of the Pegasus spyware scandals, the Supreme Court established an independent technical committee to probe into the allegation of unauthorised surveillance. Although the action was an indication of judicial gravity, the lack of a fully transparent reception restricted the effectiveness of the action on the surveillance governance in the long term.

More recently, the Digital Personal Data Protection Act, 2023, has been heralded as a milestone in India's privacy regime. Yet, its broad exemptions for government functions and limited transparency obligations have raised concerns about whether it can effectively restrain state surveillance practices. [12] Simultaneously, policy developments such as the proposed National Cyber Security Strategy and state-level facial recognition projects indicate a continuing expansion of monitoring capabilities, often without parallel institutional oversight.

Table 1: Timeline of Key Developments in India's Privacy and Surveillance Framework

Year	Event / Instrument	Significance
1963	*Kharak Singh v. State of Uttar Pradesh*	First judicial acknowledgement of aspects of privacy, though not explicitly recognised as a right.
1975	*Govind v. State of Madhya Pradesh*[13]	Introduced limited privacy protections, subject to compelling state interest.
2009	Aadhaar project launched	Began as a voluntary biometric identity scheme aimed at welfare delivery.
2016	Aadhaar Act enacted	Provided statutory basis for Aadhaar; expanded scope of linkage with services.

[10] *People's Union for Civil Liberties v. Union of India* (1997) 1 SCC 301.
[11] Bhatia, Gautam, *Offend, Shock, or Disturb: Free Speech under the Indian Constitution* (New Delhi: Oxford University Press, 2016) p. 164.
[12] Rajagopal, Krishnan, "The Data Protection Bill: Opportunities and Gaps" (2022) 64 *Journal of Indian Law and Society* 201.
[13] *Govind v. State of Madhya Pradesh* (1975) 2 SCC 148.

2017	*Justice K.S. Puttaswamy v. Union of India*	Recognised privacy as a fundamental right under Article 21; established proportionality test.
2018	*Puttaswamy (Aadhaar)* judgment	Upheld Aadhaar for welfare schemes; struck down mandatory use for private services.
2019	Aadhaar (Amendment) Act	Relaxed some restrictions, allowing voluntary use for private services under certain conditions.
2021	Pegasus spyware revelations	Triggered Supreme Court probe into allegations of unlawful surveillance.
2023	Digital Personal Data Protection Act	Established a data protection framework; criticised for broad government exemptions.

This timeline shows that while India's privacy framework has strengthened judicially, legislative and policy trends often reflect a gradual expansion of state surveillance powers. The absence of a unified, rights-oriented surveillance law means that protections remain fragmented, reactive, and heavily dependent on the political climate and public pressure.

Findings

- India does not have a single rights-based surveillance law and instead depends on outdated, fragmented provisions.
- Oversight is weak, with no independent authority to check government surveillance practices.
- The **Pegasus case** and issues with **Aadhaar** show risks of intrusive tools being used without safeguards.
- New technologies like **AFRS** and social media monitoring are being deployed without legal frameworks.
- The **Digital Personal Data Protection Act, 2023** grants broad exemptions to government use, weakening privacy rights.

Recommendations

- Enact a **comprehensive Surveillance Regulation Act** with judicial warrant requirements and strict limits.
- Create an **Independent Surveillance Commissioner** to monitor, audit, and hold agencies accountable.
- Ban or strictly regulate spyware like **Pegasus**, and strengthen Aadhaar governance with purpose limits and grievance redressal.
- Delay AFRS and similar tools until dedicated laws ensure accuracy, human oversight, and data retention limits.
- Narrow exemptions under the **DPDP Act**, enforce breach notifications, and provide strong legal remedies such as suppression of evidence and compensation.

Conclusion

Indian policy of digital government has now turned so sensitive and contested proving the election of lack of fulfillment of state to deliver safety and efficiency on one hand and government to the wings on the other hand to deliver human right fundamental to its citizens in regards to the right of privacy. The disclosures to the Aadhaar identity architecture and Pegasus spyware may individually be regarded as an outcome of a game where technology is running ahead rapidly and proper legal frameworks have not been put in place accordingly. In spite of the very fact that all of

these tools are seemingly influenced by the spirit of common good, it can be misapplied even by accommodating certain actions so that they become commonplace and will subsequently turn them into activities to facilitate the trespassing of individual lives, profiling as well as of discouraging justifiable resistance on a statistical level.

The principles of right to privacy have also found credence in the court, particularly in the case of Justice K.S. Puttaswamy where there are currently standards of legality, necessity and proportionality as guiding principles by all means of state encroachment. But these principles have been unevenly encoded in practice as coherent practice which can be deposited in their provisions. In response, such legislative texts as the Digital Personal Data Protection Act, 2023, have begun addressing the sphere of data governance, yet comprehensive governmental exceptions and slack implementation provisions grout its performance. Sympathetically, judicial interference in specific scandals, such as the Pegasus case has demonstrated institutional anxiety to challenge regimes of surveillance, though, again, has not yet resulted into any beneficial, rights-based, juridical mechanism.

The study analysis begins by stating the systematic change which is required: the development of a special law on surveillance regulations; the establishment of obligatory court sanctions of the certain surveillance; the establishment of independent apparatus of control; the adoption of the strictest systems of transparency and accountability; strict disciplinary regulations in case the illegal surveillance. The practice of other jurisdictions shows that it is simpler to apply these reforms not to mention that the need to foster the trust of people in the democratic leadership is required.