QUBAHAN POLITICAL JOURNAL
VOL. 3, NO. 1, January 2024
https://doi.org/10.48161/qpj.v3n1a14

Asymmetric Surveillance Governance: A Thematic Analysis of Privacy, National Security, and AI Regulation in India

Manu Mariyan Abraham[1], **Shampa I Dev** [1*], **Jorge Isaac Torres Manrique**[2]

[1] School of Law, CHRIST (Deemed to be) University, Bangalore 560029, India.
[2] President of the Praeeminentia Iustitia Interdisciplinary School of Fundamental Rights, Catolica Santa Maria University, Peru.
* **Corresponding author:** shampa.dev@christuniversity.in

ABSTRACT: The rapid integration of artificial intelligence into state surveillance practices has intensified longstanding tensions between consumer privacy and national security governance. In India, the enactment of the Digital Personal Data Protection Act, 2023, represents a significant regulatory development in data protection; however, its broad exemptions for state agencies raise critical constitutional and structural concerns. This paper undertakes a qualitative thematic analysis of Indian surveillance and data protection laws, supplemented by a comparative examination of regulatory frameworks in the European Union and the United States. Drawing upon statutory provisions, judicial decisions, and regulatory principles, the study identifies recurring themes including regulatory asymmetry between corporate and state actors, definitional ambiguity surrounding national security, executive-centric oversight structures, the convergence of surveillance capitalism and state data acquisition, and the algorithmic intensification of surveillance through AI systems. These themes are synthesized into a conceptual framework described as an "asymmetric surveillance governance model," in which expanded state informational power operates alongside comparatively limited institutional counterweights. The paper argues that while national security remains a legitimate constitutional objective, meaningful harmonization requires clearer definitional standards, strengthened judicial oversight, proportionality-based safeguards, and principled AI governance mechanisms. By situating India within broader comparative debates on surveillance regulation, this study contributes to ongoing scholarship on privacy, constitutionalism, and algorithmic governance in the digital state.

Keywords: consumer privacy, AI surveillance, national security, data protection law

I. INTRODUCTION

The proliferation of artificial intelligence technologies within state surveillance infrastructures has transformed the scale, speed, and sophistication of governmental data collection and analysis. From facial recognition systems and predictive policing algorithms to large-scale metadata analytics, AI-driven tools increasingly shape contemporary governance. At the same time, the exponential growth of consumer data generated through digital platforms has created vast repositories of personal information, much of which is commodified within global data markets. The intersection of these developments raises urgent constitutional and regulatory questions: how should states reconcile legitimate national security imperatives with the fundamental right to privacy in an era of algorithmic governance?

In India, the recognition of privacy as a fundamental right in Justice K. S. Puttaswamy (Retd.) v Union of India marked a watershed moment in constitutional jurisprudence, embedding proportionality as the central test for evaluating state intrusion. Subsequently, the Digital Personal Data Protection Act, 2023, introduced a statutory framework regulating private data fiduciaries and formalizing principles such as consent and purpose limitation. However, the Act simultaneously incorporates broad exemptions permitting state processing of personal data on grounds including national security, sovereignty, and public order. The Telecommunications Act, 2023, and associated interception rules further consolidate executive authority in surveillance authorization. These developments collectively produce a regulatory environment in which private actors are subject to structured

compliance obligations, while state surveillance powers operate within comparatively flexible and executive-dominated frameworks.

This paper argues that the emerging tension is not merely a doctrinal conflict between privacy and security, but a structural asymmetry embedded within the design of surveillance governance. To examine this imbalance, the study adopts a qualitative thematic analysis of statutory provisions, judicial interpretations, and comparative regulatory models, particularly the European Union's rights-based and risk-tiered approach to AI governance. By systematically identifying patterns across legal texts, the analysis develops a conceptual model of asymmetric surveillance governance, highlighting gaps in oversight, definitional clarity, and accountability mechanisms. Through this lens, the paper seeks to contribute to contemporary debates on constitutionalism in the digital age, the political economy of data, and the normative limits of AI-enabled state power.

II. RELATED WORK

Scholarly discourse on privacy and surveillance law has increasingly examined the transformation of governance structures in digitally mediated societies. Foundational theoretical frameworks conceptualize surveillance as a mechanism of social ordering and behavioral regulation, tracing its evolution from centralized institutional monitoring to decentralized and networked forms of data-driven control [1], [2]. Contemporary analyses recognize that surveillance is no longer confined to state actors but is embedded within commercial data ecosystems, where corporations collect, process, and monetize behavioral information at scale [3].

The concept of surveillance capitalism has been influential in explaining the commodification of personal data and the predictive analytics models underpinning digital platforms [4]. Legal scholars critique consent-based privacy regimes, arguing that informational asymmetries, opaque processing practices, and complex data flows undermine meaningful user autonomy [5]. The structural imbalance between data subjects and data controllers has been widely documented, with scholarship emphasizing that reliance on notice-and-consent mechanisms is insufficient to address large-scale behavioral profiling and secondary data use [6].

Parallel scholarship addresses the constitutional dimensions of state surveillance. In India, the recognition of privacy as a fundamental right in *Justice K. S. Puttaswamy (Retd.) v Union of India* established proportionality as the governing standard for evaluating privacy restrictions [7]. Academic commentary has since examined the interaction between national security exceptions and proportionality analysis, raising concerns regarding executive discretion, vague statutory standards, and limited oversight mechanisms [8]. Comparative European jurisprudence under Article 8 of the European Convention on Human Rights similarly emphasizes the importance of legality, necessity, and proportionality as essential safeguards in surveillance regimes [9].

The integration of artificial intelligence into surveillance infrastructures has further intensified these debates. Scholarship highlights risks associated with algorithmic opacity, automated profiling, biometric identification systems, and predictive policing technologies [10], [11]. The "black box" problem—where the internal logic of algorithmic systems remains opaque—poses significant challenges for transparency, accountability, and judicial review [12]. These concerns are amplified when AI systems operate within national security frameworks that already permit broad executive discretion.

Comparative regulatory analyses evaluate emerging governance models designed to address these tensions. The European Union's data protection framework under the General Data Protection Regulation (GDPR) integrates principles of purpose limitation, data minimization, and accountability, providing a structured approach to balancing innovation with fundamental rights protection [13]. In contrast, scholarship examining India's Digital Personal Data Protection Act, 2023, highlights the breadth of state exemptions and their implications for constitutional privacy guarantees [14] [15] [16] [17].

Collectively, existing literature identifies recurring concerns regarding corporate data accumulation, expansive national security justifications, and the growing influence of algorithmic systems in governance. However, these strands are often analyzed in isolation. This study contributes to the discourse by synthesizing corporate data governance, constitutional surveillance law, and AI regulation within a unified thematic framework, thereby examining how their intersection shapes contemporary surveillance governance in India and comparative jurisdictions.

III. MATERIAL AND METHOD

This study adopts a qualitative doctrinal legal research design to examine the regulatory and constitutional tensions between consumer privacy and AI-driven state surveillance. The research analyses primary legal materials, including statutory texts from India and the European Union, Supreme Court of India judgments, European human rights jurisprudence, and relevant policy documents and regulatory commentary. Primary

sources include the Digital Personal Data Protection Act, 2023; the Telecommunications Act, 2023; the Information Technology Act, 2000; the European Union Artificial Intelligence Act, 2024; the European Convention on Human Rights; and relevant case law. Secondary sources comprise peer-reviewed scholarship and policy analyses that contextualize and interpret these legal developments. The study applies a qualitative thematic analysis to identify recurring legal patterns, ambiguities, and structural tensions across jurisdictions. Using a deductive–inductive coding approach, deductive codes were derived from constitutional principles such as privacy, proportionality, and national security, while inductive codes emerged from close statutory interpretation and comparative jurisprudential analysis. Coding was systematically applied to statutory provisions, judicial decisions, comparative regulatory frameworks, and scholarly commentary. In total, the study generated 36 primary codes, organized into 12 subcategories and consolidated into 6 overarching themes, with coding conducted manually through a structured doctrinal examination of legislative and judicial texts.

Table 1. Summarized coding matrix table.

Theme	No. of Codes	Core Legal Focus
Regulatory Asymmetry	8	State vs corporate obligations
National Security Ambiguity	6	Undefined security threshold
Executive Oversight Gap	7	Lack of judicial review
Surveillance Capitalism	8	Corporate-state data nexus
AI Intensification	8	Algorithmic expansion of surveillance
Proportionality Framework	8	Constitutional balancing tools

IV. THEMATIC ANALYSIS

The thematic analysis of legislative texts, judicial decisions, and comparative regulatory frameworks reveals five interrelated structural themes that define the contemporary relationship between consumer privacy and AI-enhanced state surveillance. These themes are not isolated; rather, they operate cumulatively to shape the legal architecture governing data in India and comparable jurisdictions.

1. THEME 1: STRUCTURAL ASYMMETRY BETWEEN CORPORATE REGULATION AND STATE EXEMPTION

A central theme emerging from the doctrinal analysis is the structural asymmetry embedded within India's data protection regime. The Digital Personal Data Protection Act, 2023 (DPDPA) establishes a rights-based framework regulating "data fiduciaries," imposing duties of purpose limitation, consent, accuracy, and security safeguards. However, this regulatory discipline weakens considerably when data processing is undertaken by the state.

Sections 7(c) and 17(2)(a) of the DPDPA allow the Central Government to exempt state instrumentalities from core obligations on grounds including sovereignty, integrity, and national security. Unlike private entities, which must justify data processing through consent or legitimate use provisions, state agencies may process data non-consensually with minimal procedural transparency.

This creates a regulatory imbalance:

- Private actors are governed by structured compliance mechanisms and penalties.
- State actors are shielded by executive notifications and broad exemption clauses.

Comparatively, the European Union's General Data Protection Regulation (GDPR) permits national security exemptions under Article 23, but such exemptions must satisfy the requirements of necessity and proportionality and remain subject to judicial review. Even where national security falls within Member State competence, European Court of Human Rights (ECtHR) jurisprudence requires foreseeability and effective oversight.

The thematic divergence is clear: while India's framework reflects an intention to regulate corporate data practices, it does not embed equivalent structural accountability for state actors. This asymmetry undermines the normative claim that privacy protection is universal.

Table 2. Category a: corporate regulation (Codebook).

Code	Code Label	Description	Source Examples

CR1	Consent Requirement	Data processing based on user consent	DPDPA Section 4
CR2	Purpose Limitation	Processing is restricted to specified purpose	DPDPA framework
CR3	Data Fiduciary Duties	Obligations imposed on private entities	DPDPA compliance provisions
CR4	Penalty Mechanisms	Sanctions for corporate non-compliance	Data Protection Board powers

Table 3. Category B: state exemptions.

Code	Code Label	Description	Source Examples
SE1	National Security Exemption	Processing allowed for sovereignty/security	DPDPA Section 7(c)
SE2	Instrumentality Exemption	Government notification-based exemption	DPDPA Section 17(2)(a)
SE3	Non-Consensual Processing	Data use without data principal consent	State intelligence practices
SE4	Executive Discretion	Power vested in the executive notification	Surveillance framework

2. THEME 2: INDETERMINACY OF "NATIONAL SECURITY" AND THE SCOPE OF STATE INSTRUMENTALITY

A second recurring theme is definitional ambiguity. Neither the DPDPA nor the Telecommunications Act, 2023, provides a statutory definition of "national security." The absence of definitional clarity permits interpretative elasticity, expanding executive discretion.

Judicial precedents such as People's Union for Civil Liberties v Union of India (1997), Madhyamam Broadcasting Limited v Union of India (2023), and Manohar Lal Sharma v Union of India (2023) affirm that national security constitutes a legitimate state aim. However, the courts have simultaneously warned against blanket invocation of the term. In Puttaswamy, the Supreme Court incorporated the proportionality doctrine, requiring that state action interfering with privacy must be necessary and narrowly tailored.

Despite this jurisprudential guidance, legislative drafting remains vague. The term "state instrumentality" under Section 17(2)(a) is also undefined, leaving classification to executive notification. This introduces two layers of indeterminacy:

- The scope of national security itself.
- The institutional actors entitled to invoke it.

By contrast, under Article 8 of the European Convention on Human Rights, national security restrictions must be "in accordance with the law," meaning the law must be sufficiently clear and foreseeable. The ECtHR has repeatedly held that vague security justifications violate Article 8 protections.

The thematic concern here is not the legitimacy of national security, but the absence of normative boundaries. Indeterminacy functions as an enabling device for surveillance expansion.

Table 4. Category A: vagueness.

Code	Code Label	Description
NS1	Undefined National Security	Absence of a statutory definition
NS2	Elastic Interpretation	Broad judicial language permitting discretion
NS3	Public Order Conflation	Blurring of security and public order

Table 5. Category B: constitutional safeguards.

Code	Code Label	Description
NS4	Proportionality Test	Requirement of necessity and balancing
NS5	Legitimate Aim Doctrine	Recognition of national security as valid state interest
NS6	Limited Judicial Review	Courts deferring to executive in security matters

3. THEME 3: EXECUTIVE-CENTRIC SURVEILLANCE ARCHITECTURE AND ABSENCE OF JUDICIAL OVER-SIGHT

A third theme concerns procedural safeguards. Under the Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024, authorization and review of surveillance orders are conducted by executive authorities. Judicial approval is not mandatory at either the ex-ante or ex-post stage.

This executive-centric architecture raises concerns under the proportionality framework articulated in Puttaswamy. Effective oversight typically requires independence from the body requesting surveillance.

Comparative frameworks demonstrate stronger institutional separation:

- In several EU jurisdictions, prior judicial warrants are mandatory.
- The ECtHR has emphasized independent supervision as essential in secret surveillance regimes.
- In the United States, the Foreign Intelligence Surveillance Court (FISC) provides judicial authorization for national security surveillance.

The absence of judicial oversight in India represents a structural vulnerability. While review committees exist, their composition within the executive limits their independence.

The thematic implication is that the legality of surveillance is determined internally by the same branch of government that conducts it, thereby weakening accountability.

Table 6. Category A: executive control.

Code	Code Label	Description
EO1	Executive Authorization	Surveillance warrants issued by the executive
EO2	Executive Review Committee	Review conducted internally
EO3	No Prior Judicial Approval	Absence of ex-ante scrutiny
EO4	Administrative Confidentiality	Lack of transparency in orders

Table 7. Category B: comparative safeguards.

Code	Code Label	Description
CO1	Judicial Warrant Requirement	Mandatory court approval (EU/US)
CO2	Independent Supervisory Authority	Data protection authorities
CO3	Foreseeability Standard	Clear legal basis requirement (ECHR)

4. THEME 4: CONVERGENCE OF SURVEILLANCE CAPITALISM AND STATE DATA ACQUISITION

The thematic analysis also reveals the growing intersection between private-sector data commodification and state surveillance.

Surveillance capitalism refers to the transformation of personal data into marketable assets. Corporations collect granular behavioural data—search histories, location metadata, purchase patterns—which are monetised through targeted advertising and analytics.

The state's expanding role as a purchaser or requisitioner of commercially available data creates an indirect surveillance channel. Even if constitutional safeguards apply to direct interception, acquisition through data brokers may circumvent warrant requirements.

Scholarly literature identifies this as a "loophole" in "indiscriminate data surveillance." Governments may lawfully purchase datasets that would otherwise require judicial authorisation if directly obtained.

India's DPDPA does not explicitly regulate state procurement of brokered data. Nor does it impose warrant requirements for accessing commercially available consumer datasets.

Comparatively:

- The United States has witnessed debates on whether government purchase of location data constitutes a Fourth Amendment search.
- European jurisprudence treats mass metadata collection as falling within Article 8 scrutiny.

The thematic convergence illustrates that modern surveillance does not operate solely through traditional interception. It operates through data ecosystems in which corporate and state interests align.

Table 8. Category A: corporate data commodification.

Code	Code Label	Description
SC1	Data Monetization	Consumer data as an economic asset
SC2	Behavioural Profiling	Targeted analytics
SC3	Data Brokerage	Sale of aggregated consumer datasets
SC4	Metadata Exploitation	Use of location/search metadata

Table 9. Category B: state acquisition pathways.

Code	Code Label	Description
SA1	Brokered Government Purchase	State purchase of commercial data
SA2	Indirect Surveillance	Access without warrant
SA3	Corporate-State Convergence	Shared interest in data aggregation
SA4	Consent Bypass	The data principal is unaware of state access

5. THEME 5: AI-ENHANCED SURVEILLANCE AND EXPONENTIAL CAPACITY EXPANSION

Artificial intelligence transforms surveillance from reactive monitoring to predictive governance. AI-driven facial recognition technologies (FRT), behavioural analytics, and predictive policing tools increase both scale and depth of surveillance.

The thematic concern is not merely volume of data, but:

- Automated pattern detection
- Risk scoring
- Profiling
- Predictive intervention

AI introduces the "black box problem," where decision-making processes are opaque. This complicates accountability and judicial review.

The EU AI Act, 2024, adopts a risk-tiered model categorising AI systems as:

- Unacceptable risk
- High risk
- Limited risk
- Minimal risk

Certain biometric surveillance practices are heavily restricted or subject to strict compliance obligations.

India currently lacks AI-specific surveillance legislation. AI deployment remains governed by general executive powers under telecommunications and IT laws.

The thematic divergence between India and the EU lies in regulatory posture:

- The EU adopts a precautionary, risk-based model.
- India relies on broad administrative discretion.

AI-enhanced surveillance amplifies existing accountability gaps. Without independent oversight, AI increases the asymmetry between state capability and individual awareness.

Table 10. Category A: technological expansion.

Code	Code Label	Description
AI1	Facial Recognition Deployment	Biometric identification systems
AI2	Predictive Policing	Risk forecasting algorithms
AI3	Automated Pattern Detection	AI-driven analytics
AI4	Mass Data Scaling	Increased volume processing capability

Table 11. Category B: accountability risks.

Code	Code Label	Description
AI5	Black Box Problem	Opacity of algorithmic decisions
AI6	Algorithmic Bias	Discriminatory outputs
AI7	Explainability Deficit	Lack of transparent reasoning
AI8	Diffused Responsibility	Unclear liability allocation

6. THEME 6: THE PROPORTIONALITY PRINCIPLE AS A HARMONIZING MECHANISM

Across themes, the proportionality doctrine emerges as a potential harmonising principle. The Supreme Court in Puttaswamy established proportionality as the constitutional test for privacy interference.

However, proportionality must be operationalised through:

- Clear statutory thresholds
- Judicial warrant requirements
- Defined time limits
- Transparency obligations
- Post-surveillance notification (where feasible)

Compared with European jurisprudence, proportionality is operationalised through multi-layered safeguards.

The thematic analysis indicates that India recognises proportionality doctrinally but does not embed it structurally within surveillance procedures.

Table 12. Category A: legal balancing.

Code	Code Label	Description
PR1	Legitimate Aim	Security justification
PR2	Necessity Requirement	Least restrictive measure
PR3	Suitability Test	Rational connection
PR4	Balancing Exercise	Privacy vs security weighting

Table 13. Category B: structural safeguards.

Code	Code Label	Description
PR5	Judicial Oversight	Independent review
PR6	Time Limitation	Restricted surveillance duration
PR7	Notification Requirement	Post-surveillance disclosure
PR8	Data Minimisation	Limiting data scope

V. THEMATIC SYNTHESIS

The thematic analysis reveals a structurally embedded asymmetry within India's surveillance governance framework, characterised by the differential regulation of corporate and state actors, conceptual ambiguity surrounding national security, executive-centric authorisation mechanisms, and the accelerating impact of AI-enhanced surveillance technologies. While private data fiduciaries are subject to consent requirements, purpose limitation, and compliance obligations under the Digital Personal Data Protection Act, 2023, the state operates through broadly framed exemptions that permit non-consensual data processing on grounds that remain undefined and elastic. The absence of statutory clarity regarding "national security" and "state instrumentalities," combined with the lack of independent judicial oversight in surveillance authorisation and review processes, creates an accountability deficit within the legal architecture. This imbalance is further intensified by the convergence of surveillance capitalism and governmental data acquisition, whereby commercially brokered consumer data enables indirect state access without traditional constitutional safeguards. The deployment of AI-driven systems such as facial recognition and predictive analytics amplifies this informational asymmetry by expanding the scale, speed, and opacity of surveillance practices. Collectively, these themes illustrate not merely a tension between privacy and security, but the emergence of an asymmetric surveillance governance model in which expanded state informational power is insufficiently counterbalanced by enforceable structural safeguards.

VI. DISCUSSION

1. CONSUMER PRIVACY AND EXPANDING DATA ECOSYSTEMS

Consumer privacy concerns arise from the large-scale collection and processing of personal information by both corporations and the state. Companies routinely collect essential data necessary for service delivery—such as names, addresses, medical details, biometric verification data, and financial information. However, beyond what is strictly necessary, corporations also collect behavioral data, including search history, purchase patterns, location data, and device identifiers. This data enables targeted advertising, predictive profiling, and customized user experiences.

While consumers may perceive certain disclosures as unavoidable for service delivery, non-essential data collection has expanded significantly with AI-enabled analytics and smart technologies. Wearables, digital platforms, and predictive systems now generate continuous streams of behavioral data, increasing the economic value of personal information. Consumer data has effectively become a commercial asset.

The Consumer Protection Act, 2019 (CPA) and the Digital Personal Data Protection Act, 2023 (DPDPA) attempt to regulate misuse by classifying unauthorized disclosure of confidential information as an unfair trade practice and by defining the relationship between data principals and data fiduciaries. However, while corporate data processing is subject to regulatory safeguards, the state enjoys broad exemptions under Sections 7(c) and 17(2)(a) of the DPDPA for reasons including national security, sovereignty, and public order. These exemptions create asymmetry in privacy protection.

2. STATE SURVEILLANCE AND AI

India's surveillance framework operates under the Telecommunications Act, 2023 and the Information Technology Act, 2000. Authorization and review of surveillance activities remain within the executive branch, with no mandatory judicial oversight. The integration of AI into surveillance mechanisms significantly increases the scale, speed, and depth of monitoring.

AI-enabled tools—such as facial recognition technologies (FRT), predictive policing models, and pattern analysis systems—can process massive datasets rapidly. While such tools enhance crime prevention and national security efforts, they also intensify privacy intrusions. The Supreme Court in Manohar Lal Sharma (2023) acknowledged surveillance as a legitimate state function but cautioned against unchecked reliance on national security exemptions. In Justice K.S. Puttaswamy (2018), the Court affirmed that privacy is a fundamental right and introduced proportionality as a governing standard.

The central concern lies in vague statutory language. Terms such as "national security" and "state instrumentalities" remain undefined in the DPDPA. Without clear thresholds or objective criteria, these grounds risk arbitrary interpretation. Judicial review is limited, especially in matters involving national security, raising the possibility of unchecked executive discretion.

3. DATA LOCALISATION AND SECURITY CONCERNS

Geopolitical tensions and AI development have intensified concerns over cross-border data transfers. Allegations of foreign access to user data in applications such as TikTok and emerging AI models have led to bans and restrictions. Although the DPDPA permits the government to restrict cross-border data flows, a comprehensive localization policy remains undeveloped.

AI systems capable of accessing chat histories, biometric identifiers, and behavioral metadata raise fears of profiling, political manipulation, and surveillance beyond territorial control. Data localization is often presented as a safeguard against foreign surveillance, but without internal accountability mechanisms, localization alone does not prevent domestic misuse.

4. SURVEILLANCE CAPITALISM

The commodification of personal data has led to surveillance capitalism, where corporations collect, analyses, and monetize behavioral information. Data brokers facilitate large-scale transfers of consumer data, sometimes to government agencies. This blurs the boundary between private and state surveillance. Theoretical frameworks from Bentham's Panopticon to Foucault's disciplinary power illustrate how surveillance influences behavior through awareness of observation. Modern surveillance differs in scale and actors. Corporations and governments both accumulate data to influence markets, governance, and social control. Scholars such as Solove argue that privacy self-management is failing: individuals cannot meaningfully control or monitor how their data is collected and repurposed. Consent mechanisms are weakened by lengthy privacy policies and continuous data regeneration. Classification of "sensitive" versus "non-sensitive" data is increasingly inadequate, as aggregated metadata can reveal intimate insights.

5. POTENTIAL FOR MISUSE

The existing surveillance framework reveals several structural vulnerabilities that heighten the risk of misuse and constitutional imbalance. First, the absence of a statutory definition of "national security" permits the executive to engage in expansive, potentially subjective interpretation. Although courts have consistently recognized national security as a legitimate state aim, the proportionality doctrine requires that any restriction on privacy must satisfy standards of necessity, suitability, and minimal impairment. Without clearly defined thresholds or objective criteria, surveillance measures may extend beyond what is legitimately required. Second, Section 17(2)(a) of the DPDPA leaves the classification of "state instrumentalities" to executive notification, creating constitutional concerns

regarding administrative overreach and concentration of discretionary power. The lack of legislative clarity in determining which agencies may invoke exemptions risks arbitrary expansion of surveillance authority. Third, surveillance authorization and review remain confined to executive committees, with no mandatory involvement of the judiciary. The absence of independent judicial scrutiny at either the warrant or review stage weakens accountability and limits meaningful oversight. These structural issues are compounded by the integration of AI into surveillance mechanisms, which significantly increases the volume and speed of data collection, often exceeding operational necessity. Excessive data aggregation not only heightens privacy intrusion but may also reduce analytical precision. Furthermore, the "black box" nature of many AI systems—where decision-making processes are opaque—complicates transparency and accountability, particularly when biased training data results in discriminatory or erroneous outcomes.

VII. SUGGESTIONS

The objective is not to dismantle surveillance mechanisms but to harmonize privacy rights with legitimate state interests. Regulation should focus on structured safeguards rather than technological specifics.

1. CLEAR DEFINITIONS AND STATUTORY GUIDELINES

Legislation should define key terms such as "national security," "public emergency," and "state instrumentalities." A non-exhaustive but structured classification of agencies eligible for exemption under Section 17(2)(a) would reduce arbitrariness. Threshold criteria should require demonstrable gravity and necessity before invoking national security exemptions. Codified standards would align executive action with the proportionality principle articulated in Puttaswamy.

2. JUDICIAL OVERSIGHT MECHANISMS

Introducing judicial scrutiny at either the ex-ante (warrant authorization) or ex-post (review) stage would enhance accountability. Mandatory judicial warrants for accessing personal data under Sections 7(c) and 17(2)(a) would ensure proportionality assessment before data transfer. Judicial involvement would not eliminate surveillance but would legitimize it through independent review.

3. STREAMLINING AND EXHAUSTION REQUIREMENT

Agencies should demonstrate that they have exhausted alternative investigative methods before seeking surveillance authorization. Such a requirement, recognized in comparative human rights jurisprudence, ensures surveillance is a last resort. Surveillance orders should clearly specify scope, duration, subject, and permissible data categories to prevent overcollection. Streamlining improves efficiency and reduces unnecessary intrusion.

4. PRIVACY-BY-DESIGN IN SURVEILLANCE SYSTEMS

Privacy-by-design principles should be embedded in surveillance technologies from the earliest stages of development. Applying Ferguson's "tyrant test"—designing systems assuming potential abuse—would create structural safeguards before deployment. Built-in limitations on data retention, purpose restriction, and automated deletion protocols can reduce misuse risks.

5. PRIVACY-ENHANCING TECHNOLOGIES (PETS)

Incorporating PETs such as differential privacy, synthetic data, and homomorphic encryption can enable analytical functionality without exposing identifiable information. These technologies balance operational effectiveness with safeguards for anonymity.

6. NOTIFICATION TO DATA PRINCIPALS

A post-surveillance notification mechanism, subject to reasonable exceptions, would allow individuals to challenge unlawful data processing. Extending breach-notification principles to state actions would strengthen accountability.

7. REGULATING SURVEILLANCE CAPITALISM

Data minimization should be strictly enforced. Corporations must limit collection to what is necessary for specified purposes and avoid secondary exploitation. Regulation of data brokers is essential. Transfers of consumer

data to the government should require judicial authorization, preventing backdoor circumvention of constitutional safeguards.

8. PRINCIPLE-BASED REGULATION OF AI

Regulation should focus on what AI systems do rather than how they function technically. Structured safeguards—transparency, auditability, accountability, and oversight—should apply across technologies. A context-based risk assessment model is preferable to blanket prohibitions. Rather than classifying AI surveillance as inherently unacceptable, each surveillance order should be evaluated based on scope, objective, and risk of harm.

9. ADDRESSING THE BLACK-BOX PROBLEM

Deployment of explainable AI systems is critical for accountability. Where AI assists decision-making, human verification must remain mandatory. Independent audits and bias assessments should be institutionalized to prevent discriminatory outcomes.

10. CLARIFYING OWNERSHIP AND DATA RIGHTS

Legislative clarity is required regarding ownership of derived consumer profiles. While corporations invest resources in analytics, individuals retain fundamental rights over their personal information. Balancing proprietary interests with informational self-determination remains crucial.

VIII. CONCLUSION

There is an apparent conflict between privacy and national security imperatives. This conflict transcends its traditional setting of a tussle between privacy rights and surveillance into the modern age, AI-driven surveillance and its subsequent effects on consumer privacy. It is well established throughout the paper that there are distinguishable exemptions for the state to collect and process consumer data, especially under the national security imperative. The lack of judicial oversight or scrutiny, along with other procedural safeguards, and a hazy understanding of certain terms, creates a case for a violation of privacy rights. The paper offers specific policy recommendations, including judicial oversight, privacy-by-design principles, and privacy-enhancing technologies, to mitigate the state's intrusion into consumer privacy. Additionally, the paper takes a deep look at the emergence of surveillance capitalism and the ways in which bodies and governments are intertwined in relation to access and control over consumer data, suggesting data minimization principles and restrictions on data transfer between the two. Regarding AI-enhanced surveillance, the paper proposes a context-based approach to assessing risk and harm, while acknowledging the challenges of assigning responsibility in cases involving AI models.

The analysis undertaken in this study demonstrates that the contemporary conflict between consumer privacy and AI-driven state surveillance in India is not merely a normative tension between individual rights and collective security, but a structural imbalance embedded within the legal architecture itself. While the Digital Personal Data Protection Act, 2023, introduces meaningful regulatory obligations for private data fiduciaries, including consent requirements and compliance mechanisms, it simultaneously grants broad exemptions to the state on grounds of national security and sovereignty that are loosely defined. The absence of statutory clarity regarding key terms such as "national security" and "state instrumentalities," coupled with an executive-centric surveillance authorization process lacking independent judicial oversight, generates an accountability deficit that weakens constitutional privacy protections articulated in Justice K. S. Puttaswamy v Union of India. This imbalance is further exacerbated by the convergence of surveillance capitalism and governmental access to brokered consumer data, enabling indirect state acquisition of personal information without traditional warrant safeguards. The deployment of AI-enhanced surveillance technologies, including facial recognition and predictive analytics, intensifies these concerns by expanding the scale, opacity, and predictive capacity of surveillance systems. Comparative examination of the European Union's rights-based and risk-tiered regulatory approaches reveals the importance of structured proportionality, independent oversight, and clearly defined limitations in maintaining equilibrium between security imperatives and fundamental rights. Ultimately, the study concludes that sustainable harmonization between privacy and surveillance in India requires not the dismantling of national security mechanisms, but the institutionalization of clear definitional standards, judicial authorization procedures, proportionality-based safeguards, and principle-driven regulation of AI systems, thereby ensuring that the expansion of state informational power remains constitutionally accountable.

Funding Statement

This research received no external funding.

Author Contributions

All authors have read and agreed to the published version of the manuscript. All authors made an equal contribution to the development and planning of the study.

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability Statement

No new data were created or analyzed in this study. The research is based on publicly available legal materials.

Acknowledgments

The author acknowledges the assistance of peer reviewers and editorial feedback in refining this manuscript. The authors would like to acknowledge the use of Grammarly for improving the quality of the language.

REFERENCES

[1]. M. Foucault, Discipline and Punish: The Birth of the Prison. New York, NY, USA: Vintage Books, 1977.
[2]. G. Deleuze, "Postscript on the societies of control," October, vol. 59, pp. 3–7, 1992.
[3]. D. Lyon, Surveillance Studies: An Overview. Cambridge, U.K.: Polity Press, 2007.
[4]. S. Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York, NY, USA: PublicAffairs, 2019.
[5]. D. J. Solove, "Privacy self-management and the consent dilemma," Harvard Law Review, vol. 126, no. 7, pp. 1880–1903, 2013.
[6]. H. Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford, CA, USA: Stanford University Press, 2010.
[7]. Justice K. S. Puttaswamy (Retd.) v Union of India, (2017) 10 SCC 1 (Supreme Court of India).
[8]. A. Bhatia, "The Supreme Court's privacy judgment and the limits of the proportionality doctrine," Indian Law Review, vol. 2, no. 1, pp. 1–21, 2018.
[9]. Roman Zakharov v Russia, App. No. 47143/06, Eur. Ct. H.R. (2015).
[10]. F. Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information. Cambridge, MA, USA: Harvard University Press, 2015.
[11]. A. D. Selbst and J. Powles, "Meaningful information and the right to explanation," International Data Privacy Law, vol. 7, no. 4, pp. 233–242, 2017.
[12]. B. Friedman and H. Nissenbaum, "Bias in computer systems," ACM Transactions on Information Systems, vol. 14, no. 3, pp. 330–347, 1996.
[13]. European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation)," Official Journal of the European Union, L119, pp. 1–88, Apr. 27, 2016.
[14]. Government of India, Digital Personal Data Protection Act, 2023. New Delhi, India: Ministry of Law and Justice, 2023.
[15]. T. Suplicy Barbosa, Douglas de Castro, Anand Kumar Singh, and Salvatore Vitale, "An Experimental Assessment of AI-Based Legal Decision-Making Systems in Contract Analysis and Risk Detection", *QTJ*, vol. 5, no. 1, pp. 37–65, Jan. 2025, doi: 10.48161/qtj.v5n1a81.
[16]. Salvatore Vitale, Deepika Kulhari, and Priscila Caneparo, "AI Integration in Legal Decision-Making: Innovations and Challenges", *QTJ*, vol. 4, no. 4, pp. 29–43, Dec. 2025, doi: 10.48161/qtj.v4n4a77.
[17]. Elena E. Gulyaeva and Helen Grace D. Felix, "Impact of Digital Technologies on Legal Theory and Practice", *QTJ*, vol. 4, no. 4, pp. 12–22, Dec. 2025, doi: 10.48161/qtj.v4n4a76.