

**FROM ORWELL TO ALGORITHMS:
IS 1984 BECOMING A LEGAL REALITY?**

A LEGAL ANALYSIS OF GOVERNMENT SURVEILLANCE AND PRIVACY RIGHTS

by

Krittika Sarkar

Abstract

Contemporary digital surveillance and the expansion of state-controlled Artificial Intelligence and mass data collection have provoked anxiety about Orwellian surveillance states which Orwell's Nineteen Eighty-Four so presciently imagined. This research examines whether the situation of contemporary state surveillance creates Orwellian legal and ethical nightmares, and critiques the efficacy of legal protections for the right to privacy. Using a mixed-doctrinal and empirical approach, this paper offers an in-depth and critical analysis of the legal frameworks comprising constitutional provisions, international and regional human rights law, and case law, and correlates this with a descriptive analysis of survey data derived from an anonymous Google Forms survey with ten respondents. This research used a five-item Likert-style survey to collect data regarding the respondents' views on the expansion of surveillance, fear of data privacy, the greatest threat to privacy, the perceived sufficiency of privacy laws, and the perceived similarity of modern-day state surveillance to the year Nineteen Eighty-Four. This study found that the public believes the expansion of state surveillance is vastly evident (80%), is highly concerned about state-sponsored data privacy (70%), and is unconvinced about the sufficiency of existing state-sponsored data privacy laws (70% expressed disagreement), and that contemporary state-sponsored data privacy laws and Orwell's dystopia are highly congruent (70% expressed agreement). Data Privacy, by far, is the greatest state-sponsored surveillance concern. Within the context of proportionality and necessity within state-sponsored data privacy laws from the Puttaswamy case to the Court of Justice for the European Union and the European Court of Human Rights, this research concludes that contemporary state-sponsored data privacy laws and Orwell's Nineteen Eighty-Four, while far from perfect, are congruent and relevant.

Keywords: *government surveillance; right to privacy; digital constitutionalism; artificial intelligence; proportionality; surveillance capitalism; Nineteen Eighty-Four*

Table of Contents

Abstract.....	1
Table of Contents	2
Chapter 1: Introduction	4
1.1 Background of the Study.....	Error! Bookmark not defined.
1.2 Statement of the Problem.....	Error! Bookmark not defined.
1.3 Research Objectives.....	5
1.4 Research Questions.....	5
1.5 Scope of the Study.....	6
1.6 Significance of the Study	6
1.7 Research Hypothesis.....	6
Chapter 2: Literature Review.....	8
2.1 Government Surveillance in the Digital Age.....	8
2.2 Privacy Rights and Constitutional Protection.....	8
2.3 Digital Governance and Digital Constitutionalism.....	9
2.4 Artificial Intelligence and Facial Recognition.....	10
2.5 Big Data, Algorithmic Decision-Making, and Surveillance Capitalism.....	Error! Bookmark not defined.
2.6 Human Rights, Cyber Law, and Judicial Responses.....	11
2.7 Orwell’s Nineteen Eighty-Four as Legal and Political Reference.....	11
Chapter 3: Legal and Theoretical Framework.....	15
3.1 The Right to Privacy as a Human Right.....	15
3.2 Constitutional Protections for Privacy.....	Error! Bookmark not defined.
3.3 Proportionality and Necessity in Surveillance Law.....	Error! Bookmark not defined.
3.4 Digital Constitutionalism.....	Error! Bookmark not defined.
3.5 Surveillance Capitalism.....	Error! Bookmark not defined.
3.6 Rule of Law and Algorithmic Governance.....	Error! Bookmark not defined.
Chapter 4: Research Methodology.....	20
4.1 Research Design and Approach.....	Error! Bookmark not defined.
4.2 Population and Sample.....	Error! Bookmark not defined.
4.3 Sampling Technique	Error! Bookmark not defined.
4.4 Data Collection and Instrument.....	Error! Bookmark not defined.
4.5 Sample Size.....	Error! Bookmark not defined.
4.6 Ethical Considerations	Error! Bookmark not defined.

4.7 Data Analysis Technique.....	Error! Bookmark not defined.
<i>Note on available variables</i>	20
Chapter 5: Data Analysis and Findings	22
5.1 Respondent Profile.....	22
5.2 Question 1: Has Government Surveillance Increased in the Digital Age?	23
5.3 Question 2: Concern About the Privacy of Personal Data.....	25
5.4 Question 3: Greatest Threat to Personal Privacy	27
5.5 Question 4: Do Current Privacy Laws Adequately Protect Citizens?	28
5.6 Question 5: Does Modern Surveillance Resemble Orwell's 1984?.....	30
5.7 Overall Interpretation of the Survey.....	32
Chapter 6: Discussion	34
6.1 The Expansion of Digital Surveillance.....	34
6.2 AI-Driven Monitoring	Error! Bookmark not defined.
6.3 Government Access to Personal Data	Error! Bookmark not defined.
6.4 Privacy Rights and the Proportionality Standard	Error! Bookmark not defined.
6.5 National Security Versus Civil Liberties	Error! Bookmark not defined.
6.6 Public Trust in Surveillance Systems.....	Error! Bookmark not defined.
6.7 Does Modern Surveillance Resemble Orwell's 1984?	Error! Bookmark not defined.
6.8 Future Legal and Policy Implications	Error! Bookmark not defined.
Legal Reflection.....	39
Conclusion	41
Major Findings.....	41
Legal Implications.....	Error! Bookmark not defined.
Policy Recommendations.....	41
Limitations.....	41
Future Research	42
References	43

Chapter 1: Introduction

1.1 Background of the Study

The telescreens of Orwell's *Nineteen Eighty-Four* (1949) were Orwell's imagination of surveillance. Today, networked cameras, facial recognition, and surveillance of citizens are a part of our daily lives (Orwell, 1949). Orwell's telescreen would now be considered a primitive example of what is now a widespread, automated, digital infrastructure of surveillance, state, and supply chain. Surveillance is labor-intensive where security services are constrained by the cost of watching, Orwell's imagination would not have foreseen. Now the state and private industry have at their disposal unprecedented ability to watch citizens and supply chain in ways that would boggle the imagination of Orwell's party. This ability is not just immeasurable, but changes surveillance from mere observation to seamless, constant, and non-intrusive surveillance which guarantees the end of privacy (Zuboff, 2019).

The legal response to such a transformation has been inconsistent and slow, according to many commentators. The constitutional and human rights frameworks that provide for the protection of privacy were developed in response to a world of physical and more confined search and intrusion, and have been largely unsuccessful in providing for the protections needed in a world of digital, continuous, and pervasive ambient intrusion and surveillance. The cases of *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) and *Carpenter v. United States* (2018), as two of many examples, indicate a greater judicial awareness of these challenges and that the protection of privacy in the digital age is not solely concerned with the protection of data. However, the rate of reform in the law has still been insufficient to keep pace with the transformation of technology, and many have argued that the gap between capability and regulatory control persists (Slobogin & Brayne, 2022).

In this regard, the Orwellian analogy has gained renewed significance. In referring to 1984, it is not to argue that current liberal democracies are totalitarian in nature, but rather to show the structural components that Orwell illustrated, such as: pervasive control and observation, the collapse of the private sphere, the deterrence of opposition, and the centralization of control and power of information that are present in modern systems. For this study, the analogy is a useful tool. It explores the extent to which modern surveillance offers a legal framework that is

comparable to the one of Orwell's constructs and the extent to which current legal frameworks offer the necessary protections for privacy against such modern surveillance.

1.2 Statement of the Problem

This study analyzes the widening gap between the technological ability of the state to monitor its citizens and the law's ability to regulate such monitoring. In the interest of national security and public order, states are using artificial intelligence, facial recognition, and mass data collection. Meanwhile, the legal protections concerning the use of these technologies such as the principles of legality, necessity, and proportionality are either weak, poorly drafted, or have extensive exemptions for public officials. This results in a two-fold challenge. From a legal theory perspective, it is unknown if existing constitutional and international legal frameworks sufficiently regulate state algorithmic surveillance. From a practical perspective, it is unknown how people perceive the state of affairs regarding surveillance. This includes whether people believe that surveillance has become more pervasive, if people have confidence in the legal safeguards, and if people perceive the current situation as a more palatable version of a dystopia. This study attempts to address both challenges by integrating legal theory and empirical research concerning public perceptions.

1.3 Research Objectives

The study pursues the following objectives:

1. Studying the expansion of digital surveillance
2. Studying privacy rights in the framework of domestic and international law
3. Comparing Orwell's Nineteen Eighty-Four and present-day surveillance
4. Understanding public opinion of surveillance and privacy
5. Assessing the effectiveness of law's protective measures

1.4 Research Questions

1. In our digital world, how much has government spying increased?

2. Are the current laws on privacy enough?
3. What part do AI and algorithms play in spying on people?
4. If anything, how closely do people consider modern society to be like Nineteen Eighty-Four?
5. What is the best way the law can balance security and individual privacy?

1.5 Scope of the Study

This study utilizes a comparative and interdisciplinary methodology, incorporating elements of constitutional and cyber law, international human rights law, and legal theory, and offers a modest empirical analysis complementary to doctrinal research. The legal analysis considers sources and case law from multiple jurisdictions, especially India, the United States, and the European legal order. They were selected for their doctrinal importance, rather than for an exhaustive or extensive comparative coverage. The empirical element consists of anonymously provided responses of ten people to a five-question survey. This element is exploratory in nature, and not statistically representative. No technical analysis of the surveillance systems is done, nor is legal counsel provided. The study focuses on the scholarly analysis of the dynamically changing relationship of surveillance and privacy systems relative to the rule of law.

1.6 Significance of the Study

This research addresses the gaps in the privacy and surveillance law literature in three important ways. First, it provides a contemporary synthesis that describes the global landscape concerning the legal limits of state surveillance. This analysis shows how the doctrine of proportionality and necessity emerge as the predominant legal constraints. Second, by integrating legal doctrine with empirical research on the prevailing public attitudes, it advances the discussion on the doctrine of law and the expectations and experiences of citizens, whose trust constitutes the legitimacy of governance. Third, by analyzing the Orwellian analogy, it offers a theoretically grounded position on how the surveillance capabilities of the modern, rapidly evolving, state should be understood. The research findings will be of interest to legislators, judges, and civil society practitioners who work at the nexus of security and fundamental human rights.

1.7 Research Hypothesis

The study is organised around the following hypotheses:

H1 (Alternative Hypothesis): Expanding government surveillance and algorithmic monitoring create significant challenges to privacy rights and increasingly resemble aspects of the surveillance society portrayed in Nineteen Eighty-Four.

H0 (Null Hypothesis): Contemporary surveillance practices do not significantly undermine privacy rights and are not comparable to the surveillance model depicted in Nineteen Eighty-Four.

Due to the small sample size and the nature of the study's descriptive design, we evaluate these hypotheses through the consistency of the doctrinal analysis paired with the survey response trends, instead of formal inferential statistical methods.



Journal of Multi-Disciplinary
Legal Research

Chapter 2: Literature Review

This review aims to integrate scholarly findings published in the years 2021-2026 and related studies examining privacy and surveillance. The focus will be new studies, but foundational studies will be referenced. This review will be organized by some related themes. These themes include the rise in state surveillance, legal frameworks related to privacy, the intersection of digital governance and constitutional law, the impact of AI, facial recognition, and large-scale data and algorithmic processes, and the persistent references to Orwellian Nineteen Eighty-Four in legal and political discourse.

2.1 Government Surveillance in the Digital Age

Based on emerging scholarship, a noticeable trend has been identified concerning digital technologies modulating surveillance activities. Surveillance activities, traditionally reserved for exceptional circumstances and target specificity, have become generalized and routine. Focusing on the intersection of surveillance techniques, systems, technologies, and constitutional law, Slobogin and Brayne (2022) discuss the expansion of technologies and systems, such as closed-circuit television, automated license plate, automated facial recognition, aerial surveillance and automated body cameras, automated surveillance of individual's locations, and automated systems and technologies for data collection and surveillance. They note that the courts have slowly adapted the search doctrine to address these emerging techniques. Their findings have disclosed a perennial paradox. While the law predicates the need for judicial oversight where surveillance extends the home or the content of private communications, it is content to a much looser statutory and administrative oversight where the State collects and collates data for future access. This paradox has resulted in the extensive nature of constitutional gaps in current surveillance. This extensive nature of surveillance has resulted in a demand for legislative mechanisms that in many instances have yet to be enacted.

2.2 Privacy Rights and Constitutional Protection

One of the notable advancements in the law over the last decade has been incorporating privacy as a recognized fundamental right. In India, in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), the nine-judge bench unanimously declared privacy as part of Article 21 of the Constitution and of the rights of life and personal liberty, and described the test of restriction as a

rigorous one, having the elements of law, legitimate aim of the State and proportionality. In the United States, the Supreme Court, in *Carpenter v. United States* (2018), for the first time held that the collection of historical cell-site location information is a search under the Fourth Amendment, moving away from the third-party doctrine, and acknowledged that there should be greater scrutiny and protection of digital information. Along with the case law of the European Court of Human Rights on Article 8 of the European Convention on Human Rights, these case laws provide the structural foundation for privacy protection today and the legal frameworks to evaluate and assess the implications of surveillance today.

The European Court of Human Rights has defined many of the standards around the retention and processing of personal and biometric data. In *S. and Marper v. United Kingdom* (2008), the Grand Chamber articulated that the U.K. government's practice of retaining the fingerprints, samples, and DNA of persons who are arrested and charged but never convicted of any crime, without any time limit, violated the right to private life by its disproportionate nature. The Grand Chamber added that the practice of retaining personal data of persons who are arrested but not convicted of crimes, is a practice that requires justification. This approach developed by the Court has brought the consequences of data retention to the forefront. It is particularly relevant in the current environment where data retention has become the foundation of most data practices. This line of reasoning is later found in the decisions of the Court of Justice of the European Union (CJEU) in invalidating indiscriminate retention rules and describes the constitutional importance of the duration of surveillance and the length of time personal data are retained.

2.3 Digital Governance and Digital Constitutionalism

A larger collection of scholarship theorizes extending constitutional values to digital domains. This has been named digital constitutionalism. This scholarship addresses more of the governance of digital infrastructures created and run by states and corporations regarding the incorporation of fundamental rights and the rule of law. Scholars note that previously the global Internet made it relatively simple to exercise rights across borders. Fragmentation—both technical and regulatory—creates inequities in the exercise of rights. In some areas, like the European Union with the General Data Protection Regulation, protections have increased. In other, mostly unregulated areas, surveillance has been expanded. Digital constitutionalism, therefore, addresses the uneven tectonic and regulatory changes to digital infrastructures.

2.4 Artificial Intelligence and Facial Recognition

Regulating artificial intelligence, particularly facial-recognition technology (FRT), has been a notable area of study in the recent literature. In her study, Qandeel (2024) classifies FRT as an “unacceptable risk” AI system and claims that its usage in surveillance and policing poses a challenge to the rule of law. , FRT regulation would be required to defend human-rights principles of necessity, proportionality, and non-discrimination. The empirical studies referenced in this literature report that public surveillance facial-recognition systems were actively used in 78 countries (between 2012-2022)¹ and in many liberal democracies, not just in authoritarian regimes. The European Union’s Artificial Intelligence Act (Regulation (EU) 2024/1689) is the most sophisticated legislation so far, and classifies some biometric surveillance systems as high risk and others as prohibited, and is widely regarded as a regulatory model.

India illustrates how quickly this kind of regulatory gap can turn into practice. Since 2019 the National Crime Records Bureau has been developing a National Automated Facial Recognition System intended to give police stations across the country access to a centralised database of facial images drawn from CCTV feeds, raids, and newspaper photographs.² The Bureau has defended the project’s legality by pointing to a 2009 cabinet note approving an earlier, more limited records system, rather than to any Act of Parliament that specifically authorises facial recognition or sets limits on its use. The Internet Freedom Foundation has argued that this falls short of the first requirement the Supreme Court set out in *Puttaswamy*, namely that any restriction on privacy must rest on a clearly defined law, and that an executive notification cannot substitute for legislation.³ Unlike the European Union, which has placed real-time facial recognition by law enforcement within a specific, if contested, statutory regime under the Artificial Intelligence Act, India currently regulates the deployment of this technology by police through administrative approval alone, with no dedicated statute, no independent oversight body, and no published limits on retention or use.

2.5 Big Data, Algorithmic Decision-Making, and Surveillance Capitalism

¹ Steven Feldstein, *AI Global Surveillance (AIGS) Index* (Carnegie Endowment for International Peace, 2022 update), reporting public facial recognition systems in use in 78 of 179 countries surveyed between 2012 and 2022.

² ‘Automatic Facial Recognition System Is Made Legal by a 2009 Cabinet Note,’ Says NCRB’ (MediaNama, 14 November 2019).

³ Internet Freedom Foundation, ‘IFF’s Legal Notice to the NCRB on the Revised RFP for the National Automated Facial Recognition System’ (Project Panoptic, 2020), citing Justice K.S. Puttaswamy v Union of India (2017) 10 SCC 1 (India).

Beyond the state, the interrelation between surveillance and commerce has gained much attention. Zuboff (2019) theorizes about ‘surveillance capitalism’ and explains how private companies have developed means to commercially exploit the surveillance of citizens and the construction of ever more sophisticated and pervasive infrastructures of surveillance. These can then, and are often, adopted by the state. The convergence of state and corporate forms of surveillance means that the public authority, long considered the principal threat to individual privacy, is now of secondary concern. The relevant threat now comes from the big data and the algorithmic and automated decision-making processes that are shaping the life opportunities of citizens in ways that are both opaque and unaccountable. There is much more liquidity than in the past, the public-private divide in the literature is concerned with the surveillance of citizens. It is increasingly accepted that private data collected for commercial motives is frequently provided to the state.

2.6 Human Rights, Cyber Law, and Judicial Responses

International and regional human rights frameworks are the most significant way to address limits on surveillance systems. In *Digital Rights Ireland* (2014) and *Data Protection Commissioner v. Facebook Ireland and Schrems* (Schrems II, 2020), the Court of Justice of the European Union found the policy tools for indiscriminant data retention and transfer invalidated due to the failure of the tests of necessity and proportionality. The European Court of Human Rights examined bulk interception systems in *Big Brother Watch and Others v. United Kingdom* (2021), and found flaws in their protections. In *Glukhin v. Russia* (2023), the Court issued the first ruling in international law on the violation of the rights to private life and freedom of expression due to the implementation of highly intrusive systems of facial-recognition technology. This body of work provides clear benchmarks for the legality of different systems of surveillance.

India’s own jurisprudence on communications surveillance predates much of this European case law and remains directly relevant to the proportionality framework discussed above. In *People’s Union for Civil Liberties v Union of India*, the Supreme Court considered a challenge to section 5(2) of the Indian Telegraph Act 1885, which permits the interception of messages during a public

emergency or in the interest of public safety.⁴ The Court held that a telephone conversation held in the privacy of one's home or office is protected as part of the right to privacy under Article 21, and that interception without safeguards also infringes the freedom of speech and expression guaranteed by Article 19(1)(a). Because Parliament had not framed rules under section 7 of the Act to structure this power, the Court laid down interim procedural guidelines of its own: interception orders may be issued only by the Home Secretary of the Union or of a State, must state reasons in writing, lapse after two months unless renewed, and are subject to periodic review by a committee of senior civil servants. These guidelines were later carried into Rule 419A of the Indian Telegraph Rules 1951 and, for electronic communications, into section 69 of the Information Technology Act 2000 read with the accompanying interception rules.⁵ The result is a domestic proportionality framework built largely by judicial direction rather than legislation, a structural weakness that foreshadows the criticism, discussed later in this paper, that India's newer Digital Personal Data Protection Act 2023 leaves state surveillance largely unreformed.

2.7 Orwell's Nineteen Eighty-Four as Legal and Political Reference

In literary studies, Orwell's Nineteen Eighty-Four sets enduring rhetorical and analytical parameters for evaluating how constant watching and the breaking down of the private sphere are the most worrying aspects of today's society. When using Orwell's novel in their studies, Orwell's novel is not used as a means of literal prophecy; rather, it is a tool to identify the dangers the absence of limits on the right to surveil brings, namely the chilling of right to free speech, the collapse of the private sphere—the individual's most intimate sphere—and the imbalance of informational power between the individual and the State (Zuboff, 2019). The persistence of Orwell (and Orwellism) in law and policy suggests that Orwell will retain his relevance in focusing moral perspectives. At the same time, it should not be forgotten that the excessive use of Orwellism will lead to the loss of the unique characteristics of contemporary surveillance, which is commercially and algorithmically based. The following table summarizes the literature cited in this review.

⁴ People's Union for Civil Liberties v Union of India (1997) 1 SCC 301 (Supreme Court of India).

⁵ Information Technology Act 2000, s 69 (India); Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009 (India).

Table**1***Summary of Key Literature and Authorities Reviewed*

Author / Authority & Year	Focus / Theme	Key Contribution
Slobogin & Brayne (2022)	Surveillance & constitutional law	Documents proliferation of surveillance technologies and the uneven extension of search doctrine to pervasive techniques.
Puttaswamy v. Union of India (2017)	Constitutional privacy (India)	Affirms privacy as a fundamental right under Art. 21; establishes legality–legitimate aim–proportionality test.
Carpenter v. United States (2018)	Fourth Amendment (USA)	Holds that acquiring cell-site location data is a search, limiting the third-party doctrine for digital data.
Digital Rights Ireland (2014); Schrems II (2020)	Data retention/transfer (EU)	Invalidate indiscriminate retention/transfer for failing necessity and proportionality.
Big Brother Watch v. UK (2021)	Bulk interception (ECtHR)	Identifies deficiencies in safeguards governing bulk interception regimes under Art. 8 ECHR.
Glukhin v. Russia (2023)	Facial recognition (ECtHR)	First international judgment holding intrusive FRT incompatible with Arts. 8 and 10 ECHR.
Qandeel (2024)	AI / facial recognition regulation	Frames FRT as an unacceptable-risk AI system requiring rule-of-law regulation grounded in human rights.

Author / Authority & Year	Focus / Theme	Key Contribution
Zuboff (2019)	Surveillance capitalism	Theorises commercial extraction of behavioural data and its convergence with state surveillance.



Journal of Multi-Disciplinary
Legal Research

Chapter 3: Legal and Theoretical Framework

The study presents a series of interconnected legal theories and frameworks. The first section analyzes privacy and human and constitutional rights. Primary constraints of surveillance – the principles of proportionality and necessity – are the focus of the second section. The third section provides digital constitutionalism, surveillance capitalism, the rule of law, and algorithmic governance as the framing components of the theoretical order. The study relies on genuine and verifiable sources.

3.1 The Right to Privacy as a Human Right

Internationally, privacy is acknowledged as a fundamental human right. Article 12 of the Universal Declaration of Human Rights (1948) states that no person should be subjected to arbitrary interference with their privacy, family, home, or correspondence. Article 17 of the International Covenant on Civil and Political Rights (1966) makes this protection part of international law. Regionally, Article 8 of the European Convention on Human Rights (1950) protects a person's right to have their private and family life respected. However, this is subject to lawful interferences that are necessary and proportionate to a democratic society. Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (2000) protect private life and personal data. There is no question that privacy is a right, not a preference. The following legal research is based on the understanding that the restriction of the right to privacy must meet specific criteria and requirements.

3.2 Privacy and International Conventions

Although various methods have been adopted to incorporate international privacy standards into their legal systems, most concord with the methods used in their former colonies. India provides an example of an exception. The right to privacy was formally acknowledged in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017). In this case, a nine-judge bench situated the right to privacy within the guarantee of life and personal liberty in Article 21 and located it in the matrix of dignity and autonomy. The Court explicitly recognized that in today's world, especially in the case of the systemic violation of privacy, there is no need for a physical intrusion to compromise

privacy. In the United States, privacy is protected from the intrusion of the government through the Fourth Amendment in the context of the prohibition of unreasonable searches and has evolved from the “reasonable expectation of privacy” test articulated in *Katz v. United States* (1967) to the recognition of the constitutional protection of one’s digital footprint in *Carpenter v. United States* (2018). Despite the variation in legal systems, the right to privacy and the protection of this right in the legal system and the courts is recognized as being dependent on the evolution of technology. The distinction between recognising a right and constraining its intrusion by biometric infrastructure is drawn out further in India’s own case law on the Aadhaar programme. In *Justice K.S. Puttaswamy (Aadhaar-5J.) v Union of India*, decided the following year, a five-judge bench considered a constitutional challenge to the Aadhaar Act 2016, which links a biometric identity number, built from fingerprints and iris scans held in a single centralised database, to welfare entitlements, banking, and tax filings.⁶ A four-judge majority upheld the scheme while reading down or striking certain provisions, including the power that had allowed private companies to demand Aadhaar authentication. Writing in dissent, Chandrachud J warned that a centralised biometric database of this kind creates the structural conditions for mass surveillance regardless of the government’s stated purpose, because the technical capacity to track and profile citizens does not depend on whether that capacity is presently being misused.⁷ The disagreement between the majority and the dissent illustrates a recurring theme in this paper: courts applying an identical proportionality standard can reach opposite conclusions about the same infrastructure, depending on how much weight is given to a database’s future potential for abuse rather than its present, stated use.

3.3 Proportionality and Necessity in Surveillance Law

Ninety percent of the time when dealing with the law of state surveillance, the principles of proportionality and necessity will be of concern. Using the Puttaswamy (2017) framework, a restriction of an individual’s right to privacy would require a real and justifiable law, a real and justifiable purpose of the law, along with a real and justifiable relation of the law’s purpose to its effect. This framework has a similar structure to that found in the jurisprudence of Europe

⁶ Justice K.S. Puttaswamy (Aadhaar-5J.) v Union of India (2019) 1 SCC 1 (India).

⁷ *ibid* (Chandrachud J, dissenting).

regarding Article 8 ECHR. The proportionality and necessity framework has been applied with extreme rigor by the Court of Justice of the European Union. In *Digital Rights Ireland* (2014), the Court declared the Data Retention Directive unlawful, and in *Schrems II* (2020), the Court declared the data transfer scheme from the European Union to the United States unlawful, as it did not provide a level of protection that was, at a minimum, equivalent to the level of protection provided by the European Union. The European Court of Human Rights, in *Big Brother Watch and Others v. United Kingdom* (2021), and in *Glukhin v. Russia* (2023), applied similar scrutiny to the case of bulk interception and facial recognition, respectively. Proportionality will be the pivot on which the lawfulness of surveillance will rest.

This tension between a formally rigorous standard and its practical application is visible in India's most recent data protection legislation. Section 17(2)(a) of the Digital Personal Data Protection Act 2023 allows the Central Government to exempt any instrumentality of the State from the whole of the Act, not merely from particular obligations, on grounds such as sovereignty, security, and public order, by executive notification rather than by a reasoned, case-specific order.⁸ Commentary applying the *Puttaswamy* proportionality test to this provision has concluded that it fails the standard's later limbs: it does not require the exemption to be the least intrusive means of achieving its stated purpose, and it builds in none of the procedural safeguards, such as independent review or a defined duration, that the Court itself required for telephone interception in *PUCCL*.⁹ Civil society groups have made the same point in less technical terms, noting that the Act leaves the surveillance powers the Supreme Court criticised in 2017 conspicuously unreformed even as it regulates private data collection in detail.¹⁰ The pattern that emerges across the jurisdictions considered in this paper, namely the European Union, India, and the United Kingdom, is that state surveillance is consistently subject to a lighter procedural standard than the standard applied to comparable data collection by private actors, notwithstanding a formally identical proportionality doctrine.

3.4 Digital Constitutionalism

⁸ Digital Personal Data Protection Act 2023, s 17(2)(a) (India).

⁹ 'State Exemptions under the Digital Personal Data Protection Act, 2023: Testing Section 17(2)(a) against the Proportionality Standard' [2026] Indian Journal of Law and Legal Research 460.

¹⁰ Gayatri Malhotra, 'India's Data Protection Law Does Little for Privacy While Bolstering the State's Surveillance Powers' (Scroll.in, 26 September 2023).

Digital constitutionalism represents the goal of broadening constitutional protections—rights, power arrogation, and the rule of law—to the governance of digital infrastructures. This concept addresses a unique characteristic of the digital realm: power over the flows of information is exercised by states and private platforms. The structures of such private platforms shape the exercise of digital rights. The General Data Protection Regulation is a good example of an effort to secure constitutional protections in the digital realm, such as purpose and transfer restrictions and enforceable rights. From this perspective, the adequacy of privacy laws is determined by the frameworks of regulation and the public-private control of digital data, in addition to the constitutional texts and the judicial doctrines.

3.5 Surveillance Capitalism

According to Zuboff (2019), surveillance capitalism reinterprets the privacy problem and locates its core in the imperative of the market to harvest and profit off of behavioral data. In this model, the concern of the digital realm's pervasive surveillance is not the security of the state, but the business model that engages in the surveillance of the population in order to harvest predictive power from the raw data. The theory is important for legal scholarship, as it provides an explanation for the public-private boundary's permeability: the data structures built for commerce and socializing are the same structures the state can seize and employ for its own surveillance. Therefore, any legal scheme that addresses only the public domain will only partially solve the problem and will also leave the private domain to its devices.

3.6 Rule of Law and Algorithmic Governance

The rule of law states that the powers of the state should be exercised through legally defined, publicly promulgated, and officially enforced laws that are certain and subject to independent verification and accountability. Algorithmic governance—the delegating of important decisions to automated systems—conflicts with these demands because systems based on opaque algorithms may make governance and decision-making automated, unreviewable, and foreseeable. Qandeel (2024) argues that the use of facial recognition and other unacceptable-risk AI systems threatens

the predictability of law and the rule of law because of the systems' lack of transparency and the unchallengeability of the decisions. The combination of automated governance and surveillance presents challenges to the rule of law that go beyond a narrow definition of privacy and includes challenges to due process, the right to equality, and the structures of a democratic state. Together these frameworks provide the standards against which both the doctrinal landscape and the empirical findings are assessed.



Journal of Multi-Disciplinary
Legal Research

Chapter 4: Research Methodology

4.1 Research Design and Approach

This research utilizes a mixed method structure. In this case, the research framework integrates legal constructions and methodological frameworks using both quantitative and qualitative techniques. Once the legal constructions are identified, the second step involves the interpretation and critical evaluation of legal sources. This includes primary and secondary sources of laws, such as statutes, international and regional instruments, judicial decisions, and legal literature. The second step involves a cross-sectional survey to evaluate public perception at a certain point in time. The two methods will be integrated in the discussion section, where the findings of the survey will be used to support the legal constructions.

4.2 Population and Sample

The general population of interest includes the adult public who are able and willing to answer survey questions on the topics of surveillance and privacy. From this population, a sample of ten respondents was selected. This sample size was kept purposefully small to show the exploratory nature and purpose of this survey, as well as the sample, where the overall goal was to show the analytic nature of the study as opposed to providing support for statistical accuracy.

4.3 Sampling Technique

To complete the survey, a non-probability convenience sampling survey method was employed where the study invited accessible and interested people to complete the survey. This method, while not ideal to show a representative population concerning the study, is, in this case, an accepted method of survey implementation and was purposely kept low to show the exploratory nature of the survey with the purpose of providing qualitative support and evidence.

4.4 Data Collection and Instrument

Data were collected via an anonymous survey on Google Forms. The participant statement guaranteed voluntary response, anonymity, and that the survey served an exclusively academic purpose. The survey contained five closed-ended items: three were five-point Likert-type agreement or concern items, and the other two were categorical items. The items captured participants' perceptions of an increase in surveillance, concern for data privacy, the greatest threat

to data privacy, the sufficiency of current privacy laws, and contemporary surveillance's resemblance to Orwell's 1984.

4.5 Sample Size

The target sample size was achieved with ten respondents ($N = 10$). Each participant responded to every survey item, which resulted in no missing data. Thus, the survey data percentages are calculated based on a sample size of ten.

4.6 Ethical Considerations

The survey process adhered to typical ethical standards for the low-risk social research. The nature of the survey guaranteed that no personally identifying information was collected and each respondent was assigned a code (R1–R10). The participant statement indicated the survey's academic purpose and the researcher's intention for the survey data. Given the survey's focus on generalized perceptions, the likely risk to the participants was negligible.

4.7 Data Analysis Technique

Data were subjected to descriptive statistics for which frequency counts and percentages were assessed directly from the primary data. For each survey item, the number of respondents for each option was counted, tabulated along with the total number of respondents in the sample, and presented in a bar or pie chart, then analyzed in the context of the doctrinal framework using a legal-academic lens. Because of the small sample size and the nature of the survey, no inferential statistics were used; instead, the hypotheses were analyzed based on the observed distributions' direction and consistency.

Note on available variables

The dataset combines responses to the five substantive items with anonymized identifiers. There is no inclusion of the variables of interest such as age, gender, education, and the respondent's jurisdiction. Thus, no demographic subgroup analyses are warranted, and the respondent profile presented in the subsequent chapter relies exclusively on the response data. This absence is acknowledged in the limitations section.

Chapter 5: Data Analysis and Findings

This chapter provides an analysis of each of the ten completed surveys. For each survey item, the results are aggregated in a frequency table, and the analysis provides percentages for each item response, including a graphical distribution of the results. Each survey item result is analyzed in the context of law and legal studies. In the survey response analysis, a brief respondent profile is generated at the beginning of the item analysis. Each section of the item analysis provides the author's interpretation of the completed survey in its entirety.

5.1 Respondent Profile

Without demographic information, a descriptive profile was created based on the responses. We documented each respondent's position on the growth of surveillance (Q1) with an overall orientation recorded as "privacy protective" (respondent places concerns on the growth of surveillance and doubts the legal safeguards are sufficient, is sympathetic, and protective, of privacy) or less concerned (has a neutral stance, is reassured). We will note that the following profile is a descriptive summary of the sample and not a demographic profile.

Table

2

Respondent Profile Derived from Response Data (N = 10)

Respondent	Stance on Surveillance Expansion (Q1)	Overall Orientation
R1	Strongly Agree	Strongly privacy-protective
R2	Agree	Privacy-protective
R3	Strongly Agree	Strongly privacy-protective
R4	Agree	Moderate / mixed
R5	Strongly Agree	Strongly privacy-protective
R6	Neutral	Less concerned
R7	Agree	Privacy-protective
R8	Strongly Agree	Strongly privacy-protective

Respondent	Stance on Surveillance Expansion (Q1)	Overall Orientation
R9	Disagree	Least concerned
R10	Agree	Privacy-protective

The results suggest that a clear plurality of respondents have a privacy-oriented mindset. Eight of the ten respondents indicate surveillance systems have become more extensive in modern societies. Only respondent 9 suggests that the systems of surveillance have not expanded. The concern mostly concentrated and framed the line by line result and explained the similar worldview among respondents.



5.2 Question 1: Has Government Surveillance Increased in the Digital Age?

Table

3

Perception That Government Surveillance Has Increased in the Digital Age

Response Category	Frequency (f)	Percentage (%)
Strongly Agree	4	40
Agree	4	40
Neutral	1	10
Disagree	1	10
Strongly Disagree	0	0
Total	10	100

Figure 1. Perception that government surveillance has increased in the digital age

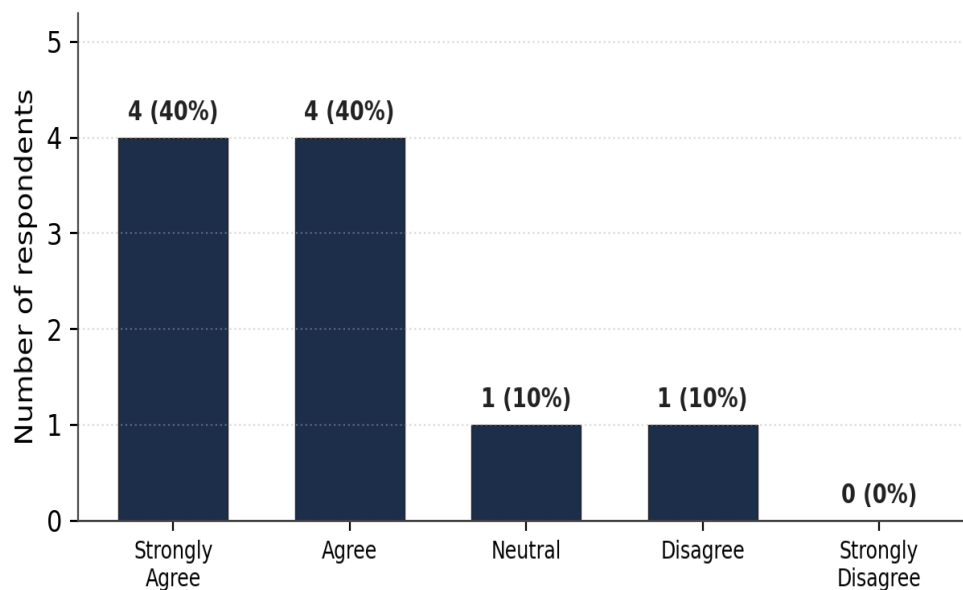


Figure 1. Perception that government surveillance has increased in the digital age (N = 10).

The first item measured consensus regarding the factual basis of the study. Respondents overwhelmingly believed that government surveillance, in the digital age, has increased. Strong agreement and agreement were expressed equally by four respondents, while one was neutral, and one was in disagreement. There were no respondents that expressed a strong disagreement. The most common responses of “Strongly Agree” and “Agree” were equally distributed, and the almost complete absence of a response is particularly noteworthy.

There is a remarkable parallelism between the perceptions of the respondents and the legal scholarship. Digital technology has changed the nature of government surveillance, and its presence in everyday life has made the practice mundane (Slobogin & Brayne, 2022). Therefore, the respondents' perception has the same legal doctrinal starting point and provides an empirical basis to its extension of the first assumption (H1). This hypothesis is based on the undisputed broadening of government surveillance.

The respondents' view, when considered in isolation, is a useful reminder that the views on government surveillance are not the same. It is possible that, from the perspective of some, there has not been an extension, and from the perspective of others, the benefits of surveillance outweigh its costs. Regardless of the perception, the majority of the responses clearly stated that, from the perspective of the respondents, government surveillance is an indisputable reality. This is the starting point of the legal analysis.

5.3 Question 2: Concern About the Privacy of Personal Data

Table

4

Level of Concern About the Privacy of Personal Data

Response Category	Frequency (f)	Percentage (%)
Very Concerned	3	30
Concerned	4	40
Neutral	1	10
Slightly Concerned	1	10
Not Concerned	1	10
Total	10	100

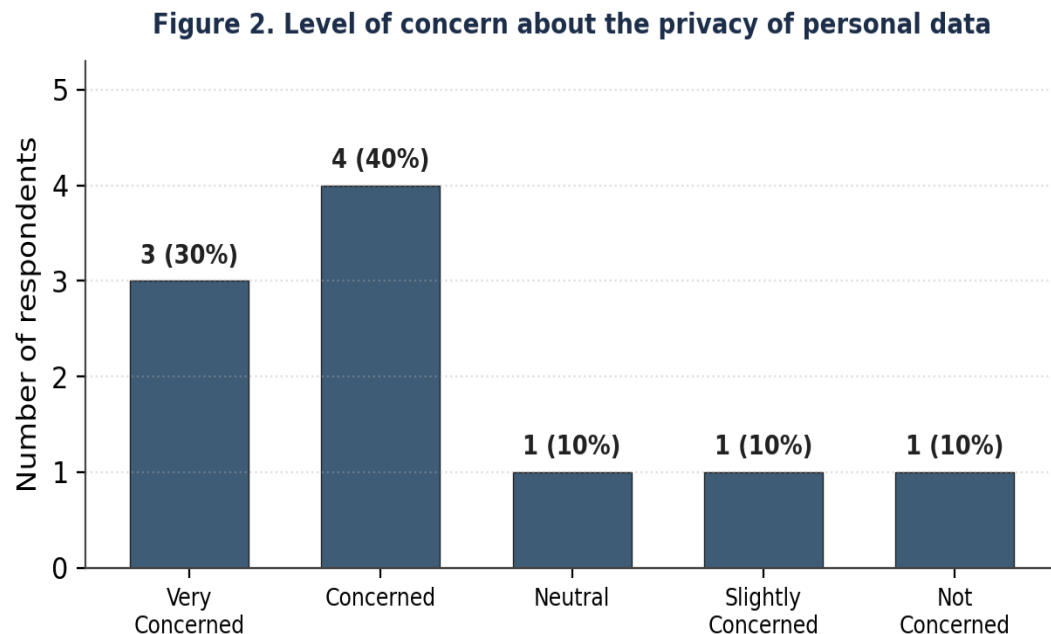


Figure 2. Level of concern about the privacy of personal data (N = 10).

The second item quantified how strongly respondents were concerned with the privacy of their personal data stored on digital platforms. In total, 70% of respondents were highly concerned, with 3 being Very Concerned and 4 being Concerned. The remaining respondents were Neutral, Slightly Concerned, and Not Concerned, at 10% each. Though having a small tail of indifference, the distribution tends to concern.

In the Puttaswamy (2017) case, the Court commented that the concern for privacy of information is more pressing today because of the invisible, systemic, and incremental modern data practices. The respondents of the survey expressed concern with the privacy of information within the data-saturated modern world with the interest in protecting the personal data from being manipulated, which is the interest of the modern jurisprudence. The respondents' concern also deals with the theory of surveillance capitalism (Zuboff, 2019). The data platforms named in the item are the data capitalists and the data platforms that Zuboff identifies as the data capitalism and surveillance capitalism of the modern data economy.

The concern of a small minority of the respondents who are not concerned should also be commented on. This may reflect the typical "nothing to hide" approach that is often seen in privacy,

or the considered approach that the data services outweigh the concerns of privacy. However, from a privacy framework, the existence of respondents that do not care about the data collection does not have a bearing on the interest of the legal framework for privacy. The concern of the majority of respondents, however, demonstrates that the respondents are supportive of the legal framework for privacy.

5.4 Question 3: Greatest Threat to Personal Privacy

Table

5

Perceived Greatest Threat to Personal Privacy

Response Category	Frequency (f)	Percentage (%)
Government surveillance	3	30
Social media platforms	2	20
Artificial Intelligence and algorithms	2	20
Cybercriminals and hackers	2	20
Data collection by private companies	1	10
Total	10	100

Figure 3. Perceived greatest threat to personal privacy

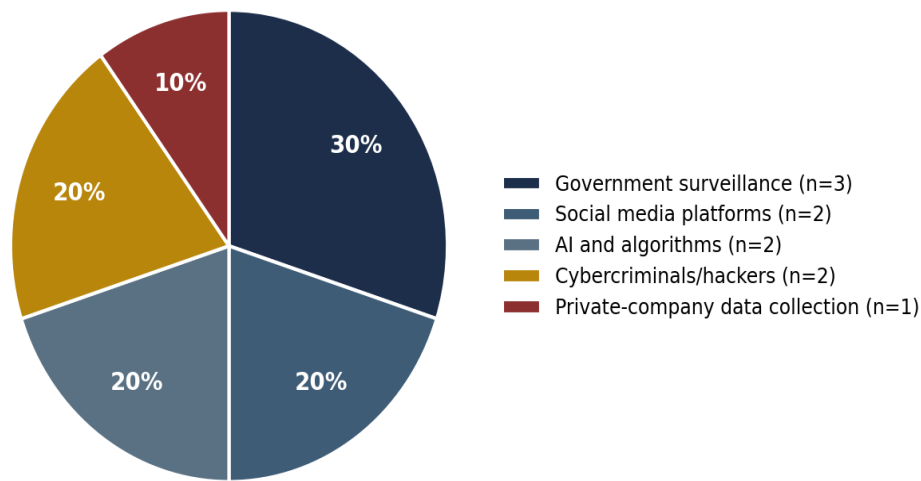


Figure 3. Perceived greatest threat to personal privacy (N = 10).

In the third question, respondents were asked to identify the most significant threat to their personal privacy. Three respondents (30%) identified government surveillance as the most significant threat. Other responses included social media companies, artificial intelligence and algorithms, cybercriminals and hackers (each identified by two respondents (20%)), and data collection by private companies (1 respondent (10%)). No threats received a majority. Responses demonstrated a clear public, private, and criminal threat dispersion.

The results regarding respondents' concerns about government surveillance are particularly interesting with the analogy to Orwell's novel. Government surveillance is at the top of the list of concerns; this result is also consistent with concerns about civil liberties that Orwell was so concerned about. However, the dispersion of the remaining responses is equally important. When social media companies, artificial intelligence and algorithms, and the data collection of private companies are considered as components of commercial and technological surveillance, these response categories collectively account for 50% of all responses, and are greater than the total concerning government surveillance. This decouples the rigid state-centric approach to privacy theories and enables an interpretation of surveillance capitalism (Zuboff, 2019), wherein commercial and state surveillance are two sides of the same coin.

Categorizing artificial intelligence and algorithms as a co-equal threat (20%) helps answer the third research question on AI and surveillance and supports the new legal scholarship that regards facial recognition and algorithmic systems as separate types of rule-of-law threats (Qandeel, 2024). Furthermore, including cybercriminals as a primary threat indicates that privacy is compromised through both legal and illegal means, and that a complete legal response must target both areas.

5.5 Question 4: Do Current Privacy Laws Adequately Protect Citizens?

Table

6

Perception That Current Privacy Laws Adequately Protect Citizens

Response Category	Frequency (f)	Percentage (%)
Strongly Agree	0	0
Agree	1	10
Neutral	2	20
Disagree	4	40
Strongly Disagree	3	30
Total	10	100

Figure 4. Perception that current privacy laws adequately protect citizens

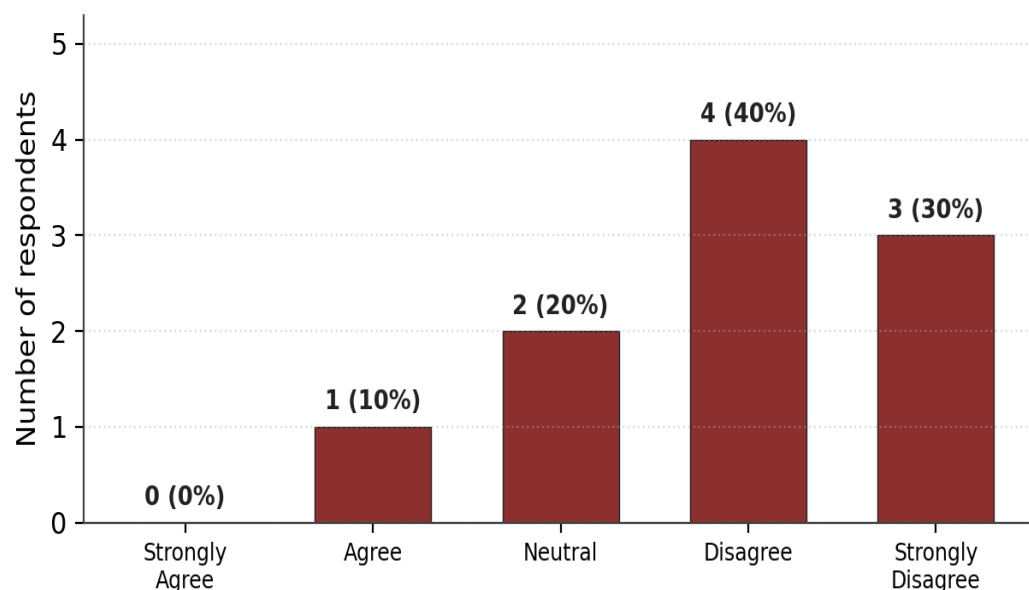


Figure 4. Perception that current privacy laws adequately protect citizens (N = 10).

The fourth item is essential, as it evaluates existing legal protections' confidence levels. The results indicate a strong negative. Of the total, 70 percent of respondents indicated a lack of confidence, comprising 10 percent of respondents that agreed with the inadequate current privacy laws, 30 percent that voted strongly, and 40 percent that voted neutrally. Only 10 percent of respondents indicated confidence with the current laws of privacy, with no respondents indicating strong agreement. Since this item requires a careful reading to decipher the key, strong disagreement indicates that there is a strong perception that the current law is inadequate.

This item constitutes the core empirical finding of this study, as it provides an answer to the second research question, and finds a highly negative public response to the sufficiency of current privacy laws. This perception corresponds with a considerable body of legal scholarship that has asserted that legal protections and laws have failed to keep pace with the advancements in technology. Slobogin and Brayne (2022) argue that important gaps exist in legal frameworks to regulate and restrict surveillance of large sets of data, and critics of legal frameworks, such as the highly broad state-actor exemptions that exist in India's Digital Personal Data Protection Act, 2023, have asserted that legal frameworks have prioritized the needs of the executive branch of government over the needs to comply with the laws of the constitution. The skepticism of the respondents is therefore grounded in legal reality, and is not mere pessimism.

This perceived inadequacy is significant from the view of the proportionality doctrine. As laid out in Puttaswamy (2017), Digital Rights Ireland (2014), and Schrems II (2020), the imposition of surveillance has to be implemented in a way that is both necessary and proportionate, with built in adequate protections. When the public has the view that laws do not provide those protections, the legitimacy of surveillance (which is based, in part, on public confidence and legal accountability) is undermined. The strength of this finding gives considerable support to the alternative hypothesis (H1), as well as the larger claim of the study, that the discrepancy between the capacity of surveillance and the limits of the law is both real and recognized by the public.

5.6 Question 5: Does Modern Surveillance Resemble Orwell’s 1984?

Table 7
Perception That Modern Surveillance Resembles Orwell’s Nineteen Eighty-Four

Response Category	Frequency (f)	Percentage (%)
Strongly Agree	4	40
Agree	3	30
Neutral	2	20

Response Category	Frequency (f)	Percentage (%)
Disagree	1	10
Strongly Disagree	0	0
Total	10	100

Figure 5. Perception that modern surveillance resembles Orwell's 1984

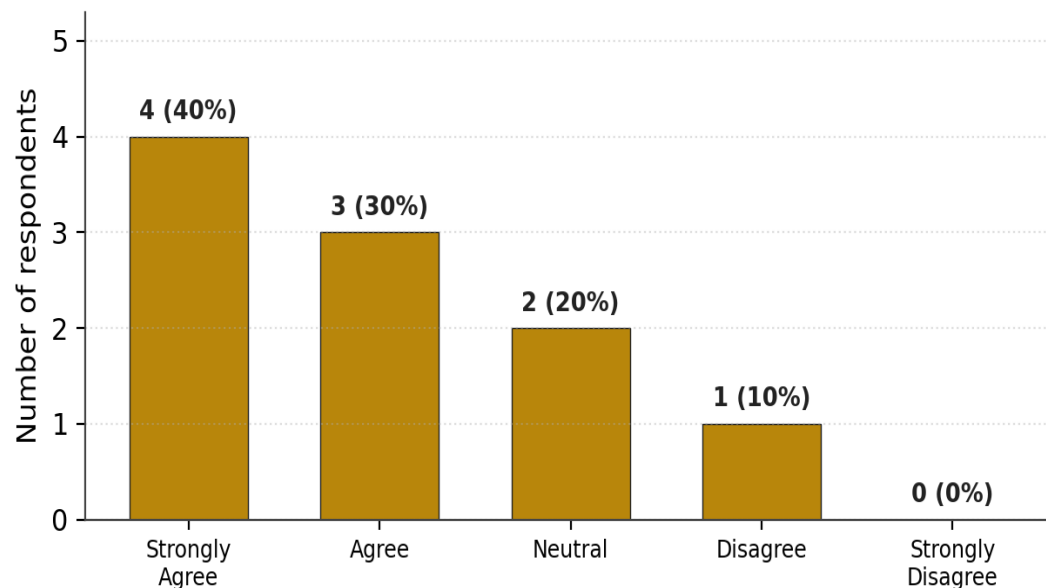


Figure 5. Perception that modern surveillance resembles Orwell's Nineteen Eighty-Four (N = 10).

The final item tested the study's primary analogy by asking whether modern day practices of surveillance mirror the society described in Orwell's Nineteen Eighty-Four. The results show that 70% of the respondents agreed or strongly agreed with the statement, with 4 respondents strongly agreeing with the statement, and 3 respondents agreeing; 2 participants were neutral, and 1 participant disagreed with the statement, and no one strongly disagreed. The results exhibit a similar distribution to the concern and the inadequacy items, indicating that the results were taken with a similar worldview.

The results of this item meet the fourth research question positively, as the majority of the respondents believe there are similarities between modern day practices of surveillance and Orwell's dystopia. This result should be interpreted with caution, as it does not mean that liberal democracies are now totalitarian. The literature rightly suggests that Orwell's dystopia should not

be used in a literal sense, as this would limit the understanding of modern day surveillance which is, in nature, commercial and highly algorithmic (Zuboff, 2019). Instead, the result of this study demonstrates that in the public's consciousness, there exists Orwell's concept of surveillance: widespread and imbalanced surveillance. The results provided by this study are in support of a hypothesis (H1) and are in support of the caution required during this analysis.

5.7 Overall Interpretation of the Survey

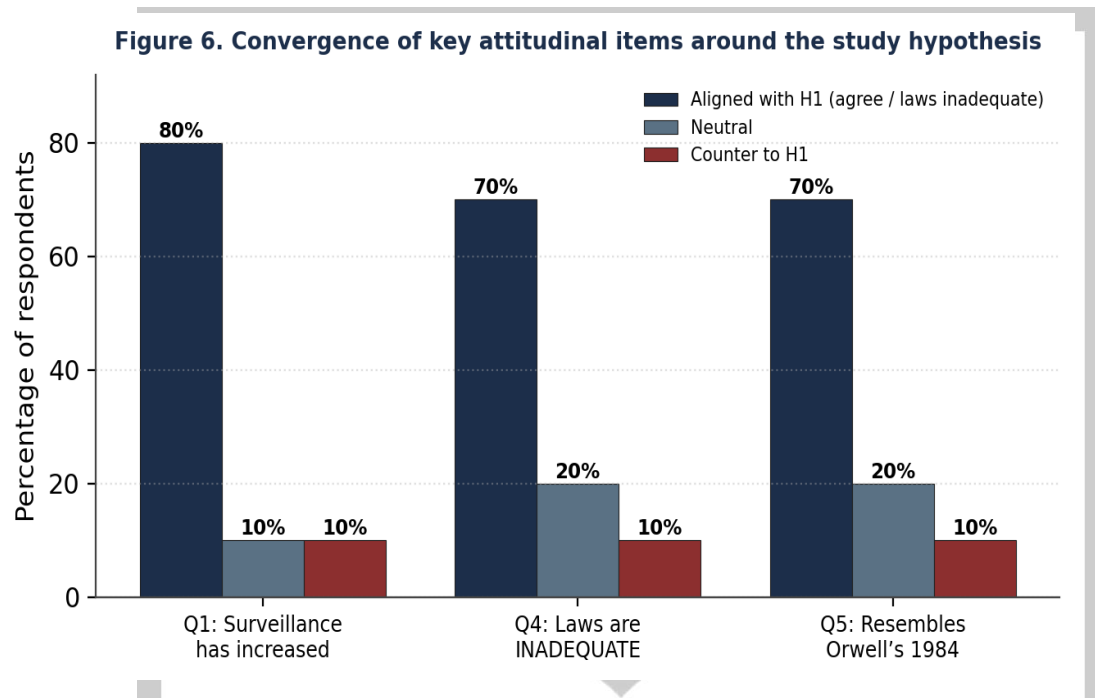


Figure 6. Convergence of key attitudinal items around the study hypothesis ($N = 10$).

The survey produces a mutually reinforcing configuration when viewed as a complete, systematic whole. Survey participants largely believe that surveillance has increased (80%, Q1) and that their concerns over the privacy of their personal data have increased (70%, Q2). When responding to Q3, participants believe that government surveillance represents the most significant disparate threat. When answering Q3, participants also believe that the majority of surveillance threats come from the private sector and the technology industry. When responding to Q4, participants largely believe that existing legal protections are insufficient (70% disagree). Finally, when responding to Q5, participants largely conclude that there are similarities to Orwell's Nineteen Eighty-Four (70%). The survey produces a cohesive understanding of the problems relating to data privacy and data surveillance for the majority of survey participants.

The first is the convergence of perceived increase of government surveillance, increased concern over the privacy of personal data, and perceived inadequate legal protections point to a legitimacy deficit. The public perceives that a powerful and uncontrolled surveillance system is growing. Second, the survey demonstrates that the public understands that government surveillance is only one side of a data collection threat, which is the public-private system of data collection. In conjunction, the survey results provide support for the first hypothesis (H1) and the rejection of the second hypothesis (H0). For the survey participants, the growing threats of surveillance are seen as a violation of the privacy rights of citizens and as a reflection of the society depicted by Orwell, although there are some limitations of the analogy, which have been discussed in the report.



Journal of Multi-Disciplinary
Legal Research

Chapter 6: Discussion

In this chapter, we look at findings from the rest of the book in light of existing legal provisions with particular reference to the expansion of digital surveillance; Artificial Intelligence-based monitoring; government access to private information; the status of privacy rights; the conflict between national security and civil rights; public confidence; the Orwell analogy; and the consequences for future law and policy.

6.1 The Expansion of Digital Surveillance

The almost universal view that surveillance is more pervasive now (Q1) converges with the doctrinal literature's description as having changed in kind, not just degree (Slobogin & Brayne, 2022). This convergence is important because it shows that the factual premises for the legal arguments are not materially disputed. Courts, theorists and the public agree that state monitoring powers have expanded significantly. The pertinent legal question is not if there has been an expansion in monitoring powers, but whether the law has been able to respond. The survey answers this question in the negative and the doctrine answers it in the partially affirmative. Proportionality jurisprudence provides a mechanism for oversight, but the case law demonstrates that this jurisprudence has been applied inconsistently across legal systems.

6.2 AI-Driven Monitoring

There is significant overlap in our respondents' answers in terms of both artificial intelligence and algorithms when it comes to potential privacy and related threats (Q3). Recent surveys have tended to agree that with the introduction of sufficiently powerful AI systems, the question of privacy and other related rights is being wholly recast. In this context, Qandeel (2024) argues that facial recognition systems represent the idea of a 'no-go zone' when it comes to balancing legal certainty with the rule of law. In a rapidly developing line of case law concerning the imposition of privacy and related rights in the EU, the European Court of Human Rights (ECtHR) has suggested that the deployment of invasive systems of facial recognition will generally be in breach of the European Convention on Human Rights. The European Union's Artificial Intelligence Act (Regulation (EU) 2024/1689) is a legislative attempt to address the threat and potential privacy violations posed by rapidly developing AI and, in particular, the use of biometric recognition systems. The results from

the survey indicate that public concern over the use of AI for surveillance and related activities is significant.

6.3 Government Access to Personal Data

The combination of government surveillance as the main single threat (Q3) and profound doubt about the legality (Q4) shifts the focus to the conditions of state access to personal data. Case law offers some guidance. In *Digital Rights Ireland* (2014) and *Schrems II* (2020), the Court of Justice of the European Union held that access to retained data should be restricted to what is strictly necessary and should be subject to independent verification. In *Big Brother Watch v. United Kingdom* (2021), the European Court of Human Rights found that the safeguards in place for bulk data collection were inadequate. In practice, the law often falls short of these standards. In the case of India's Digital Personal Data Protection Act, 2023, the criticism of broad national-security exemptions is that they can undermine the framework of so-called protections and allow the state to gain access to data with virtually no safeguards. Given this context, the respondents' doubts about the legality of the frameworks are justified.

The Pegasus controversy shows how this gap between doctrine and enforcement plays out when the technology in question is covert rather than statutory. In 2021, an international consortium of journalists reported that phone numbers belonging to Indian politicians, journalists, and activists appeared on a list linked to clients of the Pegasus spyware, which if installed can extract the entire contents of a device.¹¹ When the government declined to confirm or deny whether it had purchased or deployed the software, citing national security, the Supreme Court in *Manohar Lal Sharma v Union of India* rejected that response as insufficient and appointed an independent technical committee, overseen by a retired judge, to investigate.¹² The Court observed that even a lawful encroachment on the right to privacy must be proportionate to its purpose, and that national security cannot by itself excuse the state from accounting for its conduct before the judiciary.¹³ The episode is instructive precisely because Pegasus-style surveillance falls outside the interception framework built on *PUC*L and section 69 of the Information Technology Act

¹¹ 'Pegasus Spyware Probe: Case Background' (Supreme Court Observer, 2021).

¹² *Manohar Lal Sharma v Union of India*, Writ Petition (Crl) No 314 of 2021 (Supreme Court of India, 27 October 2021).

¹³ *ibid.*

altogether: there is no statute that visibly authorises or forbids the use of spyware of this kind, which means the ordinary proportionality safeguards this paper has traced through *Puttaswamy* and its progeny have, in practice, nothing to attach to.

6.4 Privacy Rights and the Proportionality Standard

The high level of concern for data privacy in the community (Q2) is reflected in the constitutional recognition of the right to data privacy in *Puttaswamy* (2017) and *Carpenter* (2018). The proportionality standard in *Puttaswamy* is a legal framework that requires a test of the legitimacy of the law to determine the extent to which it can be justified, balanced against competing rights. The critical factor with respect to this test is the extent to which it is applied. Where a test of proportionality has been applied with rigor, it has the potential to limit the extent of surveillance; in contrast, an application of the proportionality test that demonstrates a high degree of deference effectively becomes a mere formality. The legitimacy deficit that the survey has identified arises precisely from the gap between the rigorous standard on paper and the lack of application of this standard in practice, and it is the area in legal practice that requires the most significant reform.

6.5 National Security Versus Civil Liberties

This field exists within the framework of the balancing act between national security and civil liberties. In the name of security, states justify comprehensive spying systems. Civil proponents and judges claim security cannot justify such massive violations. Security laws attempt to address this conflict through the principles of necessity and proportionality, which claim security laws must be effective, least intrusive, and legitimized. Taking the survey results, the tightening of these laws appears to be the most important goal. In achieving this goal, the authors argue, security must be ensured, but with highly controlled measures of a more precise and independent kind.

6.6 Public Trust in Surveillance Systems

Public trust is a legal construct and element of public law because the public's faith in the system is as important as the legal accountability of state power. The survey shows a public trust deficit. People believe the state is expanding its system of surveillance and is indifferent to the state protecting people's rights. Trust deficits have legal consequences; surveillance without public consent results in the very chilling of speech and association that the Puttaswamy Court argues is a threat to democracy. The legal protections people can see and not the empty promises the government is making are essential to rebuilding trust.

The chilling effect deserves special attention as it most directly illustrates how surveillance endangers democratic existence and at what point comparisons to Orwell are most justifiable. When people think they are, or could be, watched, they alter their behavior through self-censorship, avoidance of relations with people of controversial positions, and limitation of expression, all without any direct form of coercion. The Puttaswamy (2017) Court acknowledged this situation, and held that informational privacy is a structural component of democracy, because unfettered data collection and surveillance will lead to a suppression of exercise of free speech and a suppression of the right to free association. The survey evidence of high perceived surveillance coupled with low confidence in legal protections represents the exact environment where chilling effects are most prevalent. The results are significant for more than privacy concerns. This population believes it is being watched and has no legal protections. The population's expressive and associational freedoms are constrained in a democratic society.

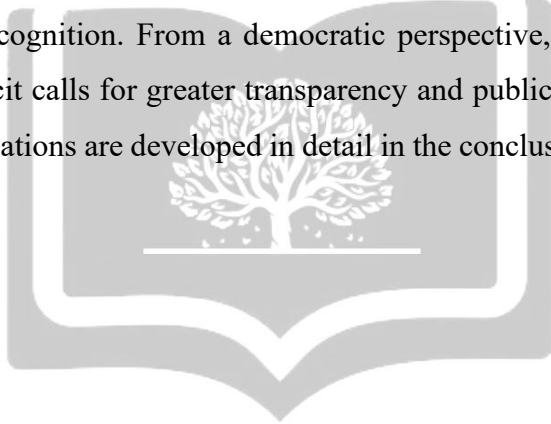
6.7. Is Surveillance Today Like Orwell's 1984?

The majority view of Orwellian resemblance (Q5) requires careful critical evaluation. There are indeed some analogies that capture structural features, such as systematic surveillance, asymmetric information, and the dampening of dissent. The analogy's structural evidence and the fact that it regularly resurfaces in both public discourse and the academic literature in this field give the analogy some validity. But there are ways the analogy fails. Orwell's Oceania was a centralised totalitarian state. Today's surveillance is decentralised, and citizens voluntarily give their data to surveillance systems in return for services. The present situation is perhaps more closely aligned with Orwell's description of a society where the totalitarian state is systematically in control, than

with a situation where the totalitarian jackboot is actively doing its worst. However, the Orwellian framework can remain useful as a normative guide and a critical frame and thinking tool, if used critically, as opposed to literally.

6.8. Implications to Law and Policy

Convergence of empirical and doctrinal studies have a number of implications. Legally, the proportionality standard must be applied more rigorously, and the law must narrow state actors' immunity and provide independent oversight and judicial control. Institutionally, the establishment of effective and independent data-protection agencies becomes essential in order to implement the constitutional principle in practice. From a technology perspective, the European Union's Artificial Intelligence Act must provide more stringent preventive (ex ante) regulations for high-risk systems, such as facial recognition. From a democratic perspective, the findings of the survey indicate that the trust deficit calls for greater transparency and public involvement in the control of surveillance. The implications are developed in detail in the conclusion, in the form of practical recommendations.



Journal of Multi-Disciplinary
Legal Research

These implications have continued to develop since the survey underlying this study was conducted. The Ministry of Electronics and Information Technology notified the Digital Personal Data Protection Rules 2025 in November 2025, bringing the 2023 Act into force, but the Rules leave the state exemption in section 17(2)(a) untouched and do not require government agencies to notify individuals when their data has been accessed under an official order.¹⁴ A constitutional challenge to both the Act and the Rules is now pending before the Supreme Court, which in February 2026 issued notice in *The Reporters Collective Trust v Union of India* and referred the underlying questions, including the Act's removal of the public-interest override from the Right to Information Act, to a larger bench, while declining for the present to stay the framework's operation.¹⁵ The outcome of that litigation will determine whether the proportionality gap this paper identifies in the survey and the doctrine alike is narrowed by judicial intervention or left for Parliament to address.

Legal Reflection

Reflecting on this material, what stands out is how quietly the architecture of surveillance has been assembled, and how far the law has trailed behind it. The great privacy judgments—Puttaswamy, Carpenter, the European jurisprudence—articulate principles of necessity and proportionality equal to the challenge; the difficulty lies in their enforcement against a technological apparatus that grows faster than doctrine can discipline it. The survey's most telling finding is not that people feel watched but that they no longer trust the law to protect them, and a rule of law that citizens perceive as failing forfeits part of its authority. Orwell's enduring relevance lies less in the accuracy of his particular dystopia than in his insight that surveillance corrodes freedom indirectly, by teaching people to censor themselves. The contemporary threat wears a gentler face than the telescreen: it is convenient, commercial, and often welcomed. Yet the chilling effect is the same, and the constitutional stakes—dignity, autonomy, and the freedom to think and associate without observation—are undiminished. The task for law is not to halt technology but to insist,

¹⁴ Digital Personal Data Protection Rules 2025 (India); 'Data Protection Rules, 2025: Critics Say It Grants Unchecked Power to the State' (The News Minute, 15 November 2025).

¹⁵ *The Reporters Collective Trust v Union of India*, Writ Petition (Civil) No 211 of 2026 (Supreme Court of India, notice issued 16 February 2026); Internet Freedom Foundation, 'Supreme Court Issues Notice on Constitutional Challenge to the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025' (2026).

unfashionably and persistently, that power over information remain answerable to principle, oversight, and the persons whose lives that information describes.



Journal of Multi-Disciplinary
Legal Research

Conclusion

Major Findings

This research aims to understand if contemporary government surveillance poses conditions similar to Orwell's Nineteen Eighty-Four and where privacy is at stake and if current privacy protections are sufficient. This research combines a doctrinal legal study and a survey of ten people, to show that government surveillance has expanded in the opinion of 80% of responders, and to show an increase in the respondents data privacy level of concern (70%), to show that government(s) surveillance is the most notable concern of a mixed public-private threat, to show that people doing surveillance has expanded in the opinion of 70% of Americans in the opinion of most Americans (70%), and to show that people privacy protection laws are actually more adequate than the opinion of 70% of Americans. In the context of the principles of proportionality, the findings support the alternative hypothesis (H1) and contradict the null hypothesis (H0).

Legal Implications

Doctrinally, the study asserts that, while flexible, law-truthful, and proportionality tests of the Puttaswamy (2017), and the necessity tests propounded by the Court of Justice of the European Union, along with the safeguard requirements of the European Court of Human Rights, do exist, but their enforcement is patchy and mostly lags behind technology. The primary concern is not the absence of law. Instead, it concerns the gap between law and practice, and is exacerbated by broad statutory immunities for state (public) actors, and the lack of clarity of algorithmic systems. Puttaswamy (2017), and the necessity tests propounded by the Court of Justice of the European Union, along with the safeguard requirements of the European Court of Human Rights.

Policy Recommendations

Here are some suggestions. To start, legislators should restrict national-security exemptions. Additionally, state surveillance should undergo independent authorization, oversight, and judicial review in line with the proportionality standard. Resources should be devoted to the establishment and strengthening of independent data-protection authorities; these entities should have the ability to implement protective measures. Additionally, some of the technologies identified as high-risk, for example, facial recognition, should be regulated in advance of use as is called for in the

European Union's Artificial Intelligence Act. Finally, transparent frameworks should be developed and maintained alongside public-participation mechanisms. Given the data from the survey, these frameworks will be necessary to rebuild the public trust in these frameworks. These suggestions balance the legitimate needs of the state when it comes to security and incorporate the right to privacy. They do not advocate prioritizing one over the other.

Limitations

This study's limitations are many. The empirical part comprises a sample of ten, which is far too small to firm any statistical generalizations. Without an array of demographics, no sub-group analysis can be run. Further, the survey captures participants' perceptions, not behaviors. The doctrinal analysis is more comprehensive in that it is cross-jurisdictional; however, it is also selective. All of these limitations require that findings are taken as suggestive only, not definitive.

Future Research

Research should utilize more substantial samples representative of different groups with demographic information to investigate how different groups understand surveillance. Research should also engage in a systematic, comparative study of the statutory protections of various jurisdictions and the enforcement of those protections; and analyze if there is a measurable chilling effect, and in what way, surveillance and other tools of social control. There is a need for studies that integrate legal doctrine with empirical social sciences and the study of technologies, to develop legal studies in the area of surveillance. Although limited in its empirical range, this study illustrates the importance of interrogating doctrine and public perception, and confirms the relevance of Orwell's Nineteen Eighty-Four, when presented with a critical, as opposed to a literal, approach. In this way, it contributes to an analysis of the legal implications of surveillance for privacy and the threats to individual freedoms and democratic accountability.

References

- Big Brother Watch and Others v. United Kingdom, App. Nos. 58170/13, 62322/14 & 24960/15 (ECtHR [GC], 25 May 2021).
- Carpenter v. United States, 138 S. Ct. 2206 (2018).
- Charter of Fundamental Rights of the European Union, 2000 O.J. (C 364) 1.
- Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems (Schrems II), Case C-311/18, ECLI:EU:C:2020:559 (CJEU, 16 July 2020).
- Digital Personal Data Protection Act, No. 22 of 2023 (India).
- Digital Rights Ireland Ltd v. Minister for Communications, Joined Cases C-293/12 & C-594/12, ECLI:EU:C:2014:238 (CJEU, 8 April 2014).
- European Convention on Human Rights, art. 8, Nov. 4, 1950, 213 U.N.T.S. 221.
- Glukhin v. Russia, App. No. 11519/20 (ECtHR, 4 July 2023).
- International Covenant on Civil and Political Rights, art. 17, Dec. 16, 1966, 999 U.N.T.S. 171.
- Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
- Katz v. United States, 389 U.S. 347 (1967).
- Orwell, G. (1949). Nineteen eighty-four. Secker & Warburg.
- People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301 (India).
- Qandeel, M. (2024). Facial recognition technology: Regulations, rights and the rule of law. *Frontiers in Big Data*, 7, 1354659. <https://doi.org/10.3389/fdata.2024.1354659>
- Regulation (EU) 2016/679 (General Data Protection Regulation), 2016 O.J. (L 119) 1.
- S. and Marper v. United Kingdom, App. Nos. 30562/04 & 30566/04 (ECtHR [GC], 4 December 2008).
- Regulation (EU) 2024/1689 (Artificial Intelligence Act), 2024 O.J. (L series).
- Slobogin, C., & Brayne, S. (2022). Surveillance technologies and constitutional law. *Annual Review of Criminology*, 6, 219–240. <https://doi.org/10.1146/annurev-criminol-030421-035102>

Solove, D. J. (2008). Understanding privacy. Harvard University Press.

Universal Declaration of Human Rights, art. 12, G.A. Res. 217A (III), U.N. Doc. A/810 (Dec. 10, 1948).

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.



Journal of Multi-Disciplinary
Legal Research