Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume:2 Issue:3
June 2025
Impact Factor:11.9
Subject: Law

BALANCING NATIONAL SECURITY AND DATA PRIVACY: A CRITICAL ANALYSIS OF SURVEILLANCE LAWS IN THE DIGITAL AGE

Kiran Shakya
PhD Research Scholar
Guest Faculty in the School of Studies in Law
Jiwaji University, Gwalior

Abstract

The need to protect national security in the era of technological surveillance and digital governance has resulted in the extension of state monitoring powers, frequently at the expense of individual privacy rights. This study critically analyses the ways in which current surveillance laws in both domestic and international jurisdictions aim to strike a balance between the protection of civil liberties and security requirements. The study assesses the moral and legal conundrums raised by the application of artificial intelligence and mass surveillance by examining important legal frameworks like the GDPR, FISA, the Investigatory Powers Act, and India's Information Technology Act. The ramifications of opaque surveillance methods, the dangers of algorithmic bias, and the disproportionate effect on underprivileged communities are also examined in the study. The study makes policy recommendations to integrate accountability, transparency, and proportionality into surveillance systems based on a comparative legal and ethical analysis. In order to guarantee that national security measures do not compromise democratic values or human dignity in the digital age, the findings highlight the urgent need for regulatory reform.

Keywords*: Digital surveillance, data privacy, national security, GDPR, ethical dilemmas, AI in surveillance, legal frameworks, human rights.*

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume:2 Issue:3
June 2025
Impact Factor:11.9
Subject: Law

1. INTRODUCTION

The spread of surveillance technologies in the modern digital age has changed the nature of civil liberties, law enforcement, and governance. The extensive use of digital surveillance tools has sparked serious concerns about the protection of individual privacy rights, even though states still have a legitimate and top priority for national security. The development of big data analytics, artificial intelligence, and cross-border data flows has made surveillance capabilities more widespread and invasive than in the past. Governments frequently use surveillance frameworks that may lack transparency, oversight, and legal accountability under the guise of maintaining security. Consequently, a notable conflict has arisen between the necessity of safeguarding national interests and the requirement to preserve fundamental human rights. This study examines the legal, ethical, and policy aspects of contemporary surveillance laws as they attempt to strike a balance between these competing goals in the digital age.

1.1.Background of the Study

In today's legal and policy discussions, striking a balance between privacy and national security has become crucial, particularly as states have increased their surveillance capacities in response to global events like pandemics, cyberwarfare, and terrorism. In reaction to security threats, surveillance laws have been passed or amended in many jurisdictions, frequently giving state agencies extensive authority without sufficient checks and balances. Concerns regarding the degradation of civil liberties have grown as a result, particularly in democracies where the right to privacy is guaranteed by the constitution. This balance has also been made more difficult by the incorporation of advanced surveillance technologies like algorithmic profiling, social media monitoring, and facial recognition. If surveillance is not adequately regulated, it can lead to discrimination, profiling, and state overreach, even though it can be extremely important in preventing crime and maintaining public safety. Thus, maintaining democratic norms in the digital age requires an awareness of the reach, consequences, and accountability of surveillance laws.

1.2.Research Objectives

The study is guided by the following research objectives:

1. To analyze international and national surveillance laws

ISSN: 2320-3714
Volume:2 Issue:3
June 2025
Impact Factor:11.9
Subject: Law

2. To examine the ethical dilemmas arising from the implementation of digital surveillance technologies.
3. To evaluate the extent of legal safeguards provided to individuals against unwarranted surveillance and data misuse.
4. To assess the role of regulatory frameworks.
5. To propose policy recommendations for achieving a balanced approach.

2. LITERATURE REVIEW

Nishat (2024) examined the complex interplay between human rights protection and digital surveillance in light of changing national security frameworks. The study underlined that while surveillance was frequently required to combat contemporary security threats, it frequently infringed upon rights guaranteed by the constitution, including freedom of expression and privacy. According to Nishat, the majority of national legal systems lacked adequate procedural protections and transparency, which allowed for the unbridled growth of surveillance. The report also suggested that domestic surveillance laws incorporate international human rights obligations, enforce proportionality standards, and incorporate judicial oversight.

Mannan (2025) explored the intricate relationship between individual liberties and national security requirements in the framework of social media regulation and digital surveillance. The study examined how governments around the world increased their surveillance capacities during the COVID-19 pandemic and after 9/11, frequently without commensurate increases in transparency or accountability. Mannan emphasised the need for precisely defined privacy rights in surveillance practices and the legal ambiguities surrounding the collection of large amounts of data. The study also examined how, in response to perceived threats, society's acceptance of surveillance frequently grew, legitimising intrusive state actions without enough public scrutiny.

Almeida, Shmarko, and Lomas (2022) carried out a comparative study of the legal, ethical, and regulatory frameworks that control surveillance and facial recognition technologies in the US, EU, and UK. The authors showed how the UK used extensive state powers under laws like the Investigatory Powers Act, the U.S. had a fragmented regulatory environment, and the EU

ISSN: 2320-3714
Volume:2 Issue:3
June 2025
Impact Factor:11.9
Subject: Law

had adopted a rights-based approach under the GDPR. The study highlighted the risks to marginalised communities, algorithmic bias, and lack of accountability that arise when AI is used for surveillance. Their conclusions reaffirmed the necessity of extensive international regulations to control cutting-edge surveillance technologies.

Andrew and Baker (2021) examined the effects of the General Data Protection Regulation (GDPR) in relation to "surveillance capitalism." They contended that although GDPR greatly enhanced data protection procedures in the EU, it was unable to control the systemic surveillance ingrained in both state-run and commercial digital infrastructures. Concerns regarding data sovereignty and user autonomy were raised by the study's revelation of how powerful entities exploited data under the pretence of consent and legal compliance. Andrew and Baker came to the conclusion that in order to successfully combat corporate and governmental overreach, GDPR needed to be enforced more strictly and harmonised internationally.

Allahrakha (2023) discussed the moral and legal difficulties in striking a balance between privacy and cybersecurity in the digital age. Many laws gave state authorities disproportionate powers under nebulous national security justifications, according to the author's critical analysis of statutory frameworks in democratic countries. According to the paper, these legal frameworks frequently undermined data privacy safeguards, making people more susceptible to invasive monitoring. To promote a more ethical and balanced surveillance ecosystem, Allahrakha suggested including explicit user consent clauses, independent audits, and data minimisation principles in national legislation.

3. ANALYSIS OF NATIONAL AND INTERNATIONAL SURVEILLANCE LAWS

Globally, surveillance laws differ greatly, reflecting varying national security priorities, technological advancements, and legal traditions. The conflict between protecting individual rights and maintaining public safety, however, never goes away. In order to comprehend how legal systems try to strike a balance between security requirements and data privacy rights, this section critically examines both international legal frameworks and national laws in a few chosen nations—the United States, the United Kingdom, and India. The common legal mechanisms, difficulties, and developing jurisprudence that influence the global surveillance landscape are also highlighted.

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume:2 Issue:3
June 2025
Impact Factor:11.9
Subject: Law

3.1.International Legal Frameworks

The right to privacy is acknowledged by international human rights law as a fundamental component of a democratic society. According to Article 17 of the International Covenant on Civil and Political Rights (ICCPR), "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home, or correspondence." However, the tenacity of this idea has been put to the test by security concerns following 9/11 and digital surveillance technologies.

The Right to Privacy in the Digital Age, a 2013 United Nations report, was a turning point in the global conversation about privacy. It demanded more robust national frameworks and oversight organisations and denounced indiscriminate mass surveillance as a breach of international human rights law.

The General Data Protection Regulation (GDPR) of the European Union, which went into effect in 2018, is regarded by many as the gold standard for data protection. It applies to both public and private organisations, requires data minimisation and purpose limitation, and offers legal recourse for improper use of data. GDPR places restrictions on the collection and use of data, including by government agencies, even though it is not a surveillance law per se.

Table 1: Key International Legal Instruments on Surveillance and Privacy

Legal Instrument	Key Provisions	Relevance to Surveillance
ICCPR, Article 17	Right to privacy; protection from arbitrary interference	Sets international legal standard for surveillance
UN 2013 Report	Surveillance must be lawful, necessary, and proportionate	Global benchmark for rights-based surveillance
European Convention on Human Rights (Article 8)	Right to respect for private and family life	Used in litigation against mass surveillance laws
EU GDPR (2018)	Regulation on data processing and protection	Restricts indiscriminate data collection

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume:2 Issue:3
June 2025
Impact Factor:11.9
Subject: Law

3.2.National Examples

❖ **United States**

The foundation of the U.S. surveillance system is a dual structure that separates the collection of national security intelligence from criminal law enforcement. The U.S. Constitution's Fourth Amendment prohibits "unreasonable searches and seizures" and mandates that most types of surveillance in criminal investigations be authorised by a judge.

However, the Foreign Intelligence Surveillance Act (FISA) of 1978 allows secret court (FISA Court) proceedings to authorise surveillance operations for national security matters. The PATRIOT Act increased federal surveillance authority after the September 11 attacks, permitting wiretapping, roving surveillance, and extensive metadata collection.

The National Security Agency (NSA) had been collecting metadata in bulk from both foreign and American citizens, according to the Snowden revelations in 2013. The USA FREEDOM Act (2015), which limited some bulk collection activities and instituted limited transparency measures, was passed as a result of the fallout from these revelations. However, detractors contend that there are still large gaps in transparency and oversight.

❖ **United Kingdom**

The Investigatory Powers Act 2016, also known as the "Snooper's Charter," largely regulates the surveillance system in the United Kingdom. This act made a number of surveillance methods legal, such as communications data retention, equipment interference (hacking), and bulk interception. Additionally, it requires internet service providers to keep records of user activity on the internet for a maximum of 12 months.

Critics argue that the Act does not meet the European Court of Human Rights' (ECHR) standard for necessity and proportionality, and it lacks sufficient judicial safeguards, despite the fact that it established the Investigatory Powers Tribunal to provide oversight and redress. A seminal case in contesting the validity of such widespread surveillance is Liberty v. UK.

❖ **India**

The Indian Telegraph Act of 1885 (Section 5) and the Information Technology Act of 2000 (Section 69) contain the majority of India's surveillance laws. In the interest of national

ISSN: 2320-3714
Volume:2 Issue:3
June 2025
Impact Factor:11.9
Subject: Law

security, public order, or sovereignty, these laws give the federal and state governments the authority to intercept, monitor, and decrypt any information. However, they rely on executive-level review committees and do not require judicial oversight.

Concerns are made worse by the absence of comprehensive privacy legislation and data protection laws. The right to privacy was deemed a fundamental right under Article 21 of the Constitution in the 2017 Supreme Court ruling in Justice K.S. Puttaswamy v. Union of India. Nevertheless, this decision has not yet resulted in tangible legislative changes to limit unbridled monitoring authority.

Table 2: Comparative Overview of Surveillance Laws in the US, UK, and India

Country	Key Laws/Acts	Oversight Mechanism	Notable Issues/Concerns
United States	FISA, PATRIOT Act, USA FREEDOM Act	FISA Court, Congressional Review	Secret courts, metadata collection, post-Snowden backlash
United Kingdom	Investigatory Powers Act 2016	Investigatory Powers Tribunal	Bulk collection, judicial review concerns
India	IT Act 2000 (Sec. 69), Telegraph Act 1885	Executive Committees	No judicial oversight, post-Puttaswamy ambiguity

Democracies differ greatly in their definitions of acceptable surveillance and data privacy protection, as these national frameworks demonstrate. India still lacks independent safeguards, which raises concerns about possible human rights violations, whereas the United States and the United Kingdom have established judicial or quasi-judicial oversight mechanisms (albeit imperfect). Furthermore, the need for flexible legal reforms and open accountability has never been greater due to the growing integration of AI and big data in surveillance systems.

4. ETHICAL AND POLICY DILEMMAS

Individual privacy and national security intersect in a profoundly ethical way that goes beyond simple legal or technical considerations. A basic ethical question is raised as governments use surveillance technologies more frequently to combat cybercrime, terrorism, and other transnational threats: How far can a government go in sacrificing individual privacy for the sake of public safety? In the digital age, where surveillance tools are more widespread, imperceptible, and potent than ever, this conundrum becomes even more complicated.

ISSN: 2320-3714
Volume:2 Issue:3
June 2025
Impact Factor:11.9
Subject: Law

4.1.The Ethics of Emergency Powers and Normalization

In times of crisis, whether it be civil unrest, pandemics, or terrorist attacks, governments frequently defend increased surveillance. These extraordinary situations usually offer moral and legal justifications for extending the state's surveillance powers. But these emergency powers often solidify and continue long after the immediate threat has subsided. This "normalisation of the exceptional" erodes democratic checks and fosters a culture of constant monitoring.

The degradation of civil liberties under the guise of security is a major ethical concern. The fundamental rights of citizens, particularly the rights to privacy, freedom of expression, and freedom of association, are threatened when surveillance measures are not clearly time-bound, necessary, and proportionate. Because they fear being watched or profiled, people may be discouraged from expressing dissent or engaging in democratic activities as a result of surveillance.

4.2.Disproportionate Impact and Surveillance Targeting

Targeting minority or marginalised groups disproportionately raises serious ethical issues as well. Surveillance systems have long been used in many nations to keep an eye on particular political, religious, or ethnic groups. This calls into question institutional bias, profiling, and discrimination. Without transparency, the use of invasive technologies can exacerbate social divisions and erode public confidence in the government.

For instance, Muslim communities in Western democracies were heavily monitored under many post-9/11 counterterrorism regimes, frequently using algorithmic profiling or ambiguous criteria. Instead of addressing actual security threats, such practices run the risk of stigmatising entire populations. It is imperative for ethical governance that surveillance not be used as a means of political control or systemic oppression.

4.3.AI, Big Data, and the Problem of Algorithmic Bias

As big data analytics and artificial intelligence (AI) grow in popularity, surveillance is becoming more automated and predictive. Law enforcement and intelligence organisations now make extensive use of technologies like social media monitoring tools, facial recognition

ISSN: 2320-3714
Volume:2 Issue:3
June 2025
Impact Factor:11.9
Subject: Law

software, and predictive policing algorithms. These tools present new ethical challenges even though they can improve security operations' efficiency.

Artificial intelligence (AI)-powered surveillance systems frequently use historical data that might have biases built in, producing discriminatory results. For example, communities that are already overpoliced may be disproportionately flagged by predictive policing systems, which would feed cycles of distrust and scrutiny. Furthermore, it is challenging for people to comprehend how they are being monitored or to contest inaccurate profiling or decisions based on AI outputs due to opaque algorithms, which are frequently shielded as proprietary technologies.

Important ethical concerns are brought up by automated surveillance systems' lack of accountability and transparency: Who creates these systems? Who conducts their audits? When they hurt someone, who bears the blame? Such technologies run the risk of becoming instruments of silent, unaccountable control in the absence of strong oversight and public input.

4.4.Policy Imperatives for Ethical Surveillance

Careful, rights-based policy interventions are needed to address these moral conundrums. Above all, the principles of necessity, proportionality, legality, and accountability must serve as the foundation for surveillance laws and practices. In order to accomplish a valid security goal, governments must make sure that any surveillance they conduct is the least invasive method possible.

Independent oversight organisations, like parliamentary committees, judicial panels, or privacy commissioners, ought to have the authority to examine surveillance practices, publish reports to the public, and serve as a check on the executive branch. To promote trust and democratic accountability, transparency requirements—such as making surveillance data and legal explanations publicly available—are crucial.

Adopting thorough data protection laws is also essential. These regulations ought to control government monitoring as well as private sector data processing, guaranteeing data minimisation, explicit purpose limitation, and channels for recourse in the event of misuse. International human rights standards must also be followed when exchanging intelligence across borders. States should not use intelligence cooperation as a way to circumvent domestic

ISSN: 2320-3714
Volume:2 Issue:3
June 2025
Impact Factor:11.9
Subject: Law

protections or to engage in "surveillance outsourcing." Instead, formal agreements that include judicial or parliamentary oversight and guarantees of data protection must govern such cooperation.

Lastly, the development of moral surveillance regulations must be heavily influenced by public discussion and civil society involvement. To make sure that surveillance does not covertly weaken society's democratic foundation, the opinions of technologists, legal experts, journalists, and human rights advocates are crucial.

5. CONCLUSION

Traditional ideas of privacy, legality, and accountability have been called into question by the digital age, which has drastically changed the nature of state surveillance. Although protecting national security is still a top priority for contemporary governments, this study has demonstrated that unbridled surveillance capabilities can undermine democratic values and violate basic human rights. Many legal systems either lack adequate oversight or do not put ethical safeguards against misuse in place, as is clear from a critical analysis of national and international surveillance laws, such as the Investigatory Powers Act, GDPR, FISA, and India's IT Act. These issues are made more complex by the incorporation of AI and predictive analytics, which introduces algorithmic bias and opaque decision-making into state monitoring procedures. Thus, it is essential to take a rights-based and balanced approach that includes independent regulatory bodies, strong data protection laws, judicial oversight, and transparency requirements. Finding this balance is ultimately a moral requirement to make sure that security does not come at the expense of personal freedom and dignity, in addition to being a legal or policy challenge.

REFERENCES

1. *Allahrakha, N. (2023). Balancing cyber-security and privacy: legal and ethical considerations in the digital age. Legal Issues in the digital Age, (2), 78-121.*
2. *Almeida, D., Shmarko, K., & Lomas, E. (2022). The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks. AI and Ethics, 2(3), 377-387.*

ISSN: 2320-3714
Volume:2 Issue:3
June 2025
Impact Factor:11.9
Subject: Law

3. *Andrew, J., & Baker, M. (2021). The general data protection regulation in the age of surveillance capitalism. Journal of Business Ethics, 168, 565-578.*
4. *Bentotahewa, V., Hewage, C., & Williams, J. (2021). Solutions to big data privacy and security challenges associated with COVID-19 surveillance systems. Frontiers in big data, 4, 645204.*
5. *Kolade, T. M., Obioha Val, O., Balogun, A. Y., Gbadebo, M. O., & Olaniyi, O. O. (2025). AI-driven open source intelligence in cyber defense: A double-edged sword for national security. Adebayo Yusuf and Gbadebo, Michael Olayinka and Olaniyi, Oluwaseun Oladeji, AI-Driven Open Source Intelligence in Cyber Defense: A Double-edged Sword for National Security(January 18, 2025).*
6. *Lund-Tønnesen, J. (2025). Privacy regimes, crisis strategies, and governments' legitimizing of digital surveillance technology: Comparing Germany, Norway, and the United Kingdom. International Journal of Public Administration, 48(5-6), 381-394.*
7. *Mannan, M. A. (2025). Surveillance and Privacy: Examining the Complex Interplay Between National Security and Individual Freedoms. In Analyzing Privacy and Security Difficulties in Social Media: New Challenges and Solutions (pp. 465-486). IGI Global Scientific Publishing.*
8. *Nair, M. M., & Tyagi, A. K. (2021). Privacy: History, statistics, policy, laws, preservation and threat analysis. Journal of information assurance & security, 16(1).*
9. *Nandy, D. (2023). Human rights in the era of surveillance: balancing security and privacy concerns. Journal of Current Social and Political Issues, 1(1), 13-17.*
10. *Nishat, K. (2024). Human Rights Protections in Digital Surveillance: Balancing Security Needs and Privacy Rights. Mayo Communication Journal, 1(1), 83-92.*
11. *Rachmad, Y. E. (2025). Privacy vs Transparency: The Regulatory Dilemma in CBDC Implementation. The United Nations and the Nobel Peace Prize Awards.*
12. *Sargiotis, D. (2024). Data security and privacy: Protecting sensitive information. In Data governance: a guide (pp. 217-245). Cham: Springer Nature Switzerland.*
13. *Westerlund, M., Isabelle, D. A., & Leminen, S. (2021). The acceptance of digital surveillance in an age of big data. Technology Innovation Management Review, 11(3), 32-44.*

ISSN: 2320-3714
Volume:2 Issue:3
June 2025
Impact Factor:11.9
Subject: Law

14. *Wheatley, M. C. Ethics of Surveillance Technologies: Balancing Privacy and Security in a Digital Age.*
15. *Williamson, S. M., & Prybutok, V. (2024). Balancing privacy and progress: a review of privacy challenges, systemic oversight, and patient perceptions in AI-driven healthcare. Applied Sciences, 14(2), 675.*

Author's Declaration

I as an author of the above research paper/article, here by, declare that the content of this paper is prepared by me and if any person having copyright issue or patent or anything otherwise related to the content, I shall always be legally responsible for any issue. For the reason of invisibility of my research paper on the website /amendments /updates, I have resubmitted my paper for publication on the same date. If any data or information given by me is not correct, I shall always be legally responsible. With my whole responsibility legally and formally have intimated the publisher (Publisher) that my paper has been checked by my guide (if any) or expert to make it sure that paper is technically right and there is no unaccepted plagiarism and hentriacontane is genuinely mine. If any issue arises related to Plagiarism/ Guide Name/ Educational Qualification /Designation /Address of my university/ college/institution/ Structure or Formatting/ Resubmission /Submission /Copyright /Patent /Submission for any higher degree or Job/Primary Data/Secondary Data Issues. I will be solely/entirely responsible for any legal issues. I have been informed that the most of the data from the website is invisible or shuffled or vanished from the database due to some technical fault or hacking and therefore the process of resubmission is there for the scholars/students who finds trouble in getting their paper on the website. At the time of resubmission of my paper I take all the legal and formal responsibilities, If I hide or do not submit the copy of my original documents (Andhra/Driving License/Any Identity Proof and Photo) in spite of demand from the publisher then my paper maybe rejected or removed from the website anytime and may not be consider for verification. I accept the fact that as the content of this paper and the resubmission legal responsibilities and reasons are only mine then the Publisher (Airo International Journal/Airo National Research Journal) is never responsible. I also declare that if publisher finds Any complication or error or anything hidden or implemented otherwise, my paper maybe removed from the website or the watermark of remark/actuality maybe mentioned on my paper. Even if anything is found illegal publisher may also take legal action against me.

Kiran Shakya

******