JOURNAL OF INTERNATIONAL LAW, POLITICS AND SOCIETY
An International Open Access Double Blind Peer Reviewed
ISSN No.: 3108-0464

Volume 2 | Issue 2 (Apr.-Jun.) | 2026 Art. 06

Balancing National Security and Privacy in Surveillance Laws: A Critical Examination of Contemporary Legal Frameworks

Utkarsh Mishra
Law Student, 5th Year, BBA.LL.B. (Hons.),
Amity Law School, Amity University, Lucknow

Recommended Citation
Utkarsh Mishra, *Balancing National Security and Privacy in Surveillance Laws: A Critical Examination of Contemporary Legal Frameworks*, 2 JILPS 81-88 (2026).
Available at www.jilps.in/current-issue/

Balancing National Security and Privacy in Surveillance Laws: A Critical Examination of Contemporary Legal Frameworks

ABSTRACT

One of the most important legal and political issues of the 21st century is the conflict between national security and privacy. Democratic governments are expanding their surveillance capabilities to combat terrorism, cyberattacks, and foreign espionage. But they run the risk of going against the constitutional freedoms that give democracy its meaning. The United States Foreign Intelligence Surveillance Act (FISA) Section 702, which was reauthorized in 2024 by the Reforming Intelligence and Securing America Act (RISAA) and is set to expire in April 2026, is the focus of this study, which looks at how contemporary surveillance law navigates and frequently struggles with this fundamental conflict. This paper argues, based on statutory analysis, judicial oversight mechanisms, comparative legal perspectives, and recent legislative history, that neither absolute privacy nor security can be achieved. What is achievable is a principled framework built on proportionality, judicial accountability, and transparent governance—one that refuses to treat security and liberty as mutually exclusive. In the paper's conclusion, a set of reform recommendations are made that have the potential to balance the effectiveness of intelligence with the protection of civil rights in a world that is being watched more and more.

KEYWORDS

FISA Section 702, Surveillance Law, National Security, Privacy Rights, Fourth Amendment, RISAA, Civil Liberties, Foreign Intelligence, Warrantless Surveillance

INTRODUCTION

In modern democracies, few policy debates are as complex as the relationship between national security and personal privacy. Governments have a fundamental responsibility to protect citizens from threats such as terrorism, organized crime, and cyberattacks. At the same time, democratic legitimacy depends on the protection of individual freedoms, including the right to privacy. The expansion of digital technology has intensified this debate because contemporary communication systems generate enormous quantities of personal data that can be monitored, stored, and analyzed by government agencies.

The growth of internet-based communication platforms has dramatically altered the nature of surveillance. Email, social media, cloud storage, and mobile networks create detailed digital records of personal interactions. Intelligence agencies may rely on these records to identify suspicious activities or detect emerging threats. Nevertheless, large-scale data collection also raises concerns about the potential misuse of government power. If surveillance activities are not subject to strict legal safeguards, they may undermine the very freedoms that democratic states are designed to protect.

The terrorist attacks of September 11, 2001 marked a turning point in surveillance policy. Governments around the world expanded their intelligence capabilities in response to the perceived need for stronger counterterrorism tools. In the United States, several new legislative measures were introduced to increase the scope of intelligence operations. Although these reforms were designed to enhance national security, they also triggered debates regarding constitutional rights, government accountability, and the limits of executive authority.

This research paper explores how modern legal frameworks attempt to reconcile security interests with privacy rights. By examining historical developments, constitutional principles, and comparative international approaches, the study aims to identify strategies that can maintain both effective intelligence operations and robust civil liberty protections.

HISTORICAL DEVELOPMENT OF SURVEILLANCE LAW

Understanding modern surveillance law requires examining the historical context in which these legal frameworks emerged. In the United States, significant concerns about government monitoring arose during the mid-twentieth century. Intelligence agencies conducted extensive surveillance of political activists, journalists, and civil rights leaders. Many of these activities were carried out without judicial authorization and were often motivated by political considerations rather than genuine security concerns.

The public awareness of these practices increased during the 1970s when the U.S. Senate established the Church Committee to investigate intelligence activities. The committee uncovered numerous instances in which federal agencies had engaged in warrantless surveillance and covert operations targeting domestic groups. These revelations generated widespread public concern and created strong political pressure for reform.

In response to these findings, Congress enacted the Foreign Intelligence Surveillance Act in 1978. The statute introduced a legal framework

designed to regulate intelligence surveillance activities conducted for national security purposes. One of its most important features was the creation of the Foreign Intelligence Surveillance Court (FISC), a specialized judicial body responsible for reviewing government surveillance requests. By requiring agencies to obtain judicial authorization before conducting certain forms of electronic monitoring, FISA attempted to establish a balance between national security needs and constitutional protections.

The legal landscape changed dramatically following the terrorist attacks of 2001. In the aftermath of these events, policymakers argued that intelligence agencies required greater flexibility to identify emerging threats. Congress responded by passing the USA PATRIOT Act, which expanded the government's ability to collect and analyze information relevant to terrorism investigations. Although supporters believed these measures were necessary to protect national security, critics expressed concerns that they could lead to excessive government intrusion into private life.

SECTION 702 AND MODERN SURVEILLANCE PRACTICES

One of the most controversial components of contemporary surveillance law is Section 702 of the Foreign Intelligence Surveillance Act Amendments Act. This provision allows intelligence agencies to collect electronic communications involving non-U.S. persons located outside the country for the purpose of acquiring foreign intelligence information. Unlike traditional surveillance warrants, which require a court order for each specific target, Section 702 operates through programmatic authorization.

Under this system, the government submits general targeting and minimization procedures to the Foreign Intelligence Surveillance Court for approval. Once these procedures are authorized, intelligence agencies may collect communications that fall within the approved parameters. This approach allows analysts to monitor foreign actors more efficiently, particularly in cases involving rapidly evolving security threats.

Despite its operational advantages, Section 702 has generated considerable debate among legal scholars and civil liberties organizations. Because global communication networks are highly interconnected, surveillance targeting foreign individuals may incidentally capture communications involving U.S. citizens. These communications are stored in intelligence databases and may later be searched during investigations. Critics argue that such searches could effectively allow domestic surveillance without traditional judicial warrants.

Supporters of the program contend that Section 702 has played an important role in identifying terrorist networks, preventing cyberattacks, and monitoring foreign intelligence activities. They emphasize that oversight mechanisms—including internal compliance reviews and judicial supervision by the Foreign Intelligence Surveillance Court—are designed to prevent misuse. Nevertheless, policymakers continue to debate whether additional safeguards are necessary to protect privacy rights.

CONSTITUTIONAL CONSIDERATIONS

The legal debate surrounding surveillance powers is closely connected to the Fourth Amendment of the United States Constitution. The Fourth Amendment protects individuals from unreasonable searches and seizures and requires that warrants be issued only upon probable cause. Historically, courts have interpreted this provision using several legal doctrines, including the third-party doctrine.

According to the third-party doctrine, individuals may lose certain privacy protections when they voluntarily share information with external service providers. For example, telephone numbers dialed through a telephone company were historically considered accessible to law enforcement because they were disclosed to the service provider during the normal course of communication. While this reasoning made sense in earlier technological contexts, it has become increasingly controversial in the digital era.

Modern communication systems involve continuous interaction with digital platforms that store vast quantities of personal information. Emails, location data, financial transactions, and social media interactions are routinely processed by private companies. If the third-party doctrine were applied strictly to all such data, government agencies could potentially access extensive personal information without obtaining traditional search warrants.

In *Carpenter v. United States (2018)*, the Supreme Court recognized the need to reconsider earlier assumptions about privacy in the digital age. The Court ruled that law enforcement generally must obtain a warrant before accessing historical cell-site location data from mobile carriers. Although the decision did not eliminate the third-party doctrine entirely, it demonstrated judicial willingness to adapt constitutional interpretation to evolving technological realities.

NEED FOR REFORM

Oversight investigations have revealed several instances in which

surveillance authorities were used improperly or without adequate factual justification. These findings have intensified calls for reform among lawmakers, civil liberties advocates, and legal scholars. While most observers acknowledge the importance of intelligence gathering, many argue that stronger safeguards are necessary to prevent misuse.

One widely discussed reform proposal involves requiring judicial approval before intelligence agencies conduct searches involving U.S. persons within Section 702 databases. Proponents believe such a requirement would reinforce constitutional protections while preserving the operational value of the program. Opponents argue that mandatory warrants could slow intelligence analysis and reduce the program's effectiveness during urgent national security investigations.

Another emerging concern relates to the commercial data market. Private data brokers collect large amounts of personal information about individuals, including location data and online behavior patterns. Government agencies may purchase such information directly from these brokers. Critics argue that this practice allows agencies to obtain sensitive personal data without complying with the legal standards that would apply if they requested the information from telecommunications companies. As a result, several legislative proposals have suggested regulating government purchases of commercial data.

COMPARATIVE INTERNATIONAL PERSPECTIVES

Examining surveillance laws in other democratic jurisdictions provides valuable insights into alternative regulatory approaches. The European Union, for example, has adopted a comprehensive data protection regime through the General Data Protection Regulation (GDPR). This legal framework recognizes privacy as a fundamental right and imposes strict requirements on organizations that collect or process personal data. Individuals are granted rights to access, correct, and erase their personal information, and organizations must demonstrate lawful justification for data processing activities.

The United Kingdom has adopted a different approach through the Investigatory Powers Act 2016. This statute explicitly authorizes several intelligence techniques while introducing a system that combines executive approval with judicial oversight. Government ministers may authorize certain surveillance measures, but these decisions are subject to review by independent judicial commissioners. Supporters argue that this "double-lock" mechanism provides accountability while allowing intelligence agencies to operate effectively.

Although these systems differ in structure, they share a common

objective: ensuring that surveillance powers remain subject to legal supervision and democratic accountability. Comparative analysis suggests that effective oversight institutions and transparent legal frameworks are essential components of responsible intelligence governance.

CONCLUSION

The expansion of digital surveillance technologies has created new challenges for legal systems across the world. Governments must protect citizens from evolving security threats while preserving the civil liberties that define democratic societies. Achieving this balance requires carefully designed legal frameworks that provide intelligence agencies with necessary operational tools while imposing meaningful limits on the exercise of state power.

This research paper has examined the historical evolution of surveillance law, the constitutional principles governing privacy rights, and the contemporary debates surrounding intelligence authorities such as Section 702. The analysis demonstrates that the relationship between security and privacy should not be viewed as a simple trade-off. Instead, democratic societies must strive to protect both values simultaneously.

Future reforms should focus on strengthening judicial oversight, increasing transparency regarding surveillance practices, and ensuring that emerging technologies are governed by clear legal standards. Through continuous legislative review and public engagement, it is possible to develop surveillance policies that maintain national security while respecting the fundamental rights of individuals.

REFERENCES

- "Data, Surveillance and Privacy in the Digital State" *The Guardian*.
- "Debate Over FISA Section 702 Renewal Intensifies" *The New York Times*.
- Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (W.W. Norton, 2015).
- *Carpenter v. United States*, 585 U.S. (2018).
- Christopher Slobogin, "Government Surveillance and the Fourth Amendment" (2015) 72 *Washington and Lee Law Review* 1485.
- Daniel J. Solove, *Nothing to Hide: The False Tradeoff Between Privacy and Security* (Yale University Press, 2011).
- European Commission, *General Data Protection Regulation (GDPR) Implementation Report* (2020).
- Foreign Intelligence Surveillance Act, 1978 (USA).
- Jack M. Balkin, "The Constitution in the National Surveillance State" (2008) 93 *Minnesota Law Review* 1.
- *K.S. Puttaswamy v. Union of India* (2017) 10 SCC 1.
- *Katz v. United States*, 389 U.S. 347 (1967).
- Laura K. Donohue, "Section 702 and the Collection of International Telephone and Internet Content" (2014) 38 *Harvard Journal of Law & Public Policy* 117.
- Neil Richards, *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age* (Oxford University Press, 2015).
- Orin S. Kerr, *The Fourth Amendment and New Technologies* (Cambridge University Press, 2021).
- Paul M. Schwartz, "Information Privacy in the Cloud" (2013) 161 *University of Pennsylvania Law Review* 1623.
- Ryan Calo, "Artificial Intelligence Policy: A Primer and Roadmap" (2017) 51 *UC Davis Law Review* 399.
- UK Investigatory Powers Commissioner's Office, *Annual Report on Surveillance Oversight* (latest edition).
- United Nations Human Rights Council, *The Right to Privacy in the Digital Age* (2018).
- USA PATRIOT Act, 2001 (USA).
- Woodrow Hartzog & Frederic Stutzman, "The Case for Online Obscurity" (2013) 101 *California Law Review* 1.