LEGAL LOCK JOURNAL

2583-0384

VOLUME 4 || ISSUE 3

2025

Striking the Balance: National Security vs. Privacy Rights in the Age of Surveillance

Likitha Sri Meka[1] & Rupam Banerjee[2]

Abstract

National security and individual privacy have been central to the salient issue brought about by growing reliance on surveillance in governments' efforts to counter all sorts of threats today, such as terrorism, cybercrime, or espionage. From a legal point of view and from ethical aspects, and within practical contexts, international norms, constitutional safeguards, as well as landmark judicial decisions, will dominate the balance given to the right of surveillance against the right to privacy.

The research will be multidisciplinary in approach, analyzing legal frameworks, case law, and comparative studies from jurisdictions such as India, the United States, and the European Union. It evaluates the effectiveness of surveillance mechanisms while critiquing their impact on fundamental rights, including the right to privacy as recognized under Article 21 of the Indian Constitution and Article 8 of the European Convention on Human Rights.

As made known by the research, surveillance can be a necessity to national security, yet its exercise uncontrolled has, at times, been interpreted to mean abuse, undermining the faith of the people in their institutions and democracy. Issues for the surveillance regimes cited include lack of transparency, oversight by the courts, and proportionality.

Above everything, a strong legal system that guarantees accountability, transparency, and proportionality is essential. Recommendations would be the passing of comprehensive data protection legislations, the creation of independent monitoring institutions, and making people aware of their privacy rights. The need to strike an optimal fine balance between security arrangements within democratic nations without undermining the very nature of individual freedoms is the seriousness brought out in this research.

Keywords

Surveillance, Privacy, National Security, Right to Privacy, Data Protection, Cybersecurity

[1] The author is a student of law at Symbiosis Law School, Hyderabad.
[2] The Co Author is a student of law at Manipal Law School, Bengaluru.

Introduction

Surveillance is organized observation of groups or individuals. It is a very potent tool in the hands of the government, as well as institutions, to provide security, enforce laws, and ward off potential threats. Privacy, on the other hand, is the natural right to exercise control over personal information and seek refuge from undeserved intrusion[3]. Therefore, conflict between surveillance and privacy reflects fundamental in modern governance, especially in an era of rapidly changing technologies and increasing world-wide interconnectivity[4].

Its usefulness has expanded exponentially in the internet era, when information is wealth literally. Governments everywhere, with terror, cyber crimes, and espionage on the cards, have increased surveillance. Facial recognition, data mining, and mass electronic surveillance are some of the tools used for that[5]. Even here, balance between accountability of information and security serves to enhance fears of misuse, abuse of power, and erosion of civil liberties[6].

This is seen in the scandals that have preceded government programs such as PRISM in the US and India's expanded granting of access to information through channels such as Aadhaar[7]. The pro-surveillance movement associates it with national security, where it is used to protect citizens from harm. Critics believe that unless curbed, surveillance leads to a surveillance state in which it erodes democratic values and treads on the basic rights of citizens.

The conflict lies in striking a balance between personal privacy and national security. Should either be overly emphasized, the cost is horrific—either on the basis of public safety or at the expense of personal freedom. This article discusses this balance through the investigation of the most applicable legal frameworks, ethical concerns, and seminal judicial decisions in order to address an imperative question of our time: How do societies balance the requirement for security with the obligation to protect privacy in a way that is democratic?

[3] *Samuel D. Warren & Louis D. Brandeis, The Right to Privacy*, 4 Harv. L. Rev. 193, 205 (1890).
[4] Daniel J. Solove, *Understanding Privacy* 1–2 (2008).
[5] David Lyon, *Surveillance After Snowden* 12–15 (2015).
[6] Shoshana Zuboff, *The Age of Surveillance Capitalism* 9–11 (2019).
[7] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India) (Aadhaar case)

Review of Literature

The balance between surveillance laws and privacy rights has been extensively debated in legal and academic literature. This paper, then, lingers on the evolving interrelation between state security concerns and human freedoms. Most seminal contributions of scholars, judgments by courts, and international sources have been considered here to indicate the prevailing shortcomings and the distinguishing angle of this paper.

Surveillance and Legal Frameworks

The development of surveillance legislation in various jurisdictions has been extensively researched by legal authors. Lawrence Lessig and Daniel Solove's publications identify the necessity of regulating government surveillance to avoid abuse of power[8]. Lessig's theory of "code as law" emphasizes how technology systems, such as surveillance programs, can enforce rules without using conventional legal oversight[9]. Solove's investigation into the "nothing to hide" argument critiques the justification often employed to defend the legality of mass surveillance[10]. However, such research tends to confine itself within certain jurisdictions rather than giving an all-round comparison of comparative legal frameworks.

The Right to Privacy

Such authors as Samuel Warren and Louis Brandeis have been found to describe privacy as "the right to be let alone.[11]" More recent works of Justice A.P. Shah point out that the issue was all the more critical in the digital age, which has been further buttressed by judgments such as Justice K.S. Puttaswamy v. Union of India[12]. While that is the case, there remains a lack of discussion on how privacy rights are to be protected in the face of surging development of surveillance technologies.

Judicial Views and Case Study

[8] Lawrence Lessig, *Code and Other Laws of Cyberspace* 6–9 (Basic Books rev. ed. 2006).
[9] Id.
[10] Daniel J. Solove, *Nothing to Hide: The False Tradeoff Between Privacy and Security* 1–4 (Yale Univ. Press 2011).
[11] Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193, 195 (1890).
[12] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India)

Judgment is a requirement to fathom the relationship between privacy and surveillance. If there were to be landmark judgments of Klayman v. Obama (USA)[13], Digital Rights Ireland v. Minister for Communications (EU)[14] Justice K.S. Puttaswamy (India), that would have helped clear judicial thoughts. Vikram Raghavan and David Cole argued that the proportionality and necessity tests play an important role in determining whether the surveillance is legitimate or not. However, the studies mentioned lack an interdisciplinary approach that has to do with ethics and technology perspectives.

International Human Rights Frameworks

The Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR) enshrine privacy as a fundamental human right. Regional instruments, such as the European Convention on Human Rights (ECHR), provide further protection through Article 8[15]. Christof Heyns and Martin Scheinin have discussed how these instruments apply to ensure a balance between privacy and surveillance[16]. However, they rarely touch on the lack of enforcement mechanisms in international law, which leaves considerable gaps in accountability.

Ethical Issues in Surveillance

Ethical debates on surveillance often talk about utility, considering a greater good. Sources from Jeremy Bentham, as construed by contemporary thinkers, tend to underscore the balancing act between personal rights and group security. Deontology, for example, as put forward by Immanuel Kant, respects the "inviolability of privacy." While such ethical theories provide a theoretical background, practical solutions need to take into account legal considerations.

Technological Issues

[13] Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013).
[14] Digital Rights Ireland Ltd. v. Minister for Communications, Joined Cases C-293/12 & C-594/12, EU:C:2014:238 (Apr. 8, 2014).
[15] Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 221, art. 8.
[16] Christof Heyns & Martin Scheinin, Report of the UN Special Rapporteurs on the Right to Privacy in the Digital Age, U.N. Doc. A/HRC/34/60 (Mar. 15, 2017).

AI and big data introduced a new challenge in surveillance practices. Some writers such as Shoshana Zuboff criticized the "surveillance capitalism" phenomenon, where data meant for security purposes is exploited for commercial reasons. The literature indicates that clarity and accountability in the application of technology are lacking, however, the detailed analysis of legal response to these issues is still lacking.

The Gaps

Despite great strides in understanding legal, ethical, and technological aspects of surveillance and privacy, a number of gaps still prevail. First, there is hardly any comparative research that compares surveillance practices and privacy protections across different legal systems. Second, the emerging technologies and their interplay with legal safeguards have not been explored adequately, especially in the AI-driven context of surveillance. Existing literature largely overlooked the socio-political impacts, such as fueling inequality and the discrimination of the vulnerability groups, regarding surveillance.

This paper aims to fill these gaps by adopting a holistic, multidisciplinary approach. It integrates legal, ethical, and technological perspectives to analyze the impact of surveillance on privacy rights. The study offers a global perspective by comparing practices in jurisdictions such as India, the United States, and the European Union. It considers the implications of emerging technologies, and recommendations will be given concerning legal and policy reforms that guarantee security and abide by democratic tenets.

This paper fills this gap and joins the ongoing conversation about finding that balance between national security and privacy, hence providing actionable information for policymakers, legal practitioners, and scholars.

Method

It goes on to detail the intricate aspects of legal and socio-political dimensions that constitute the conflict over national security vs. privacy rights, particularly on surveillance issues. The study bases itself on an examination of case law, statutory law, international treaties, and judicial doctrine that have created the shaping landscape for surveillance and privacy. Additionally, the

socio-legal impacts of new tools of surveillance such as facial recognition are examined in an effort to expose their ramifications on civil liberties as well as democratic government.

The courts' decisions are central in legal thinking in the matters of surveillance and privacy. An important case in the United States used to assess the constitutionality of bulk surveillance programs, such as the National Security Agency's collection of telephone metadata under the USA PATRIOT Act, is ACLU v. Clapper (2015). The American Civil Liberties Union argued before the Supreme Court that it was a Fourth Amendment ban on unreasonable searches and seizures. In this case, the Supreme Court ruled that bulk collection of phone records by the NSA as conducted was not in accordance with the Fourth Amendment. The case ultimately was dismissed on procedural grounds, so the issues were left hanging about how the balance between national security and privacy rights would be struck.

In India, the decision of Justice K.S. Puttaswamy v Union of India (2017) adjudged privacy as a constitutional right according to Article 21 of the Indian Constitution. It related to the constitutional validity of the Aadhaar Act that enabled the state to procure the biometric identity of its citizens. The Supreme Court of India held that, even as privacy was a constitutional right, the state could restrict it in the interest of national security, subject to the conditions that such restrictions satisfy the tests of necessity, proportionality, and fairness. This judgment serves as a barometer to weigh the right to privacy against the security of the state under the gaze of surveillance.

Digital Rights Ireland Ltd. v. Minister for Communications (2014) in the European Union was a judicial ruling on the tension between surveillance and privacy. The CJEU has ruled the Data Retention Directive as illegitimate under the European Union's Charter of Fundamental Rights since it breached its principles in that the aforementioned directive obligated telecommunication providers to retain metadata concerning users. To this end, the CJEU held that bulk data retention violated charter rights to privacy because such an intervention is not necessary for the maintenance of national security. The ruling also emphasized proportionality and necessity principles relating to surveillance measures within the EU.

Some domestic laws and international agreements provide statutory frameworks for weighing privacy claims against national security claims. The USA PATRIOT Act of 2001 is among the most remarkable legislation laws in the U.S. used after the September 11 attacks to strengthen national security. The Act broadly authorized surveillance by government agencies while the FBI and NSA can examine private information without a warrant in certain cases. Yet certain of its stipulations- specifically, the collection of metadata and foreign communications spying-have been faulted for being invading private rights to privacy.

In contrast, the General Data Protection Regulation that European Union implemented, as of 2018, concerns the protection of personal data of natural persons and mandates strict data processing regulations encompassing both private and public. The GDPR mandates explicit consent for data collection and grants rights to individuals to access, correct, and delete their personal data. While the GDPR does allow for exceptions in national security and law enforcement situations, the exceptions are narrowly crafted to guarantee that privacy rights are not unfairly sacrificed to surveillance activities.

The International Covenant on Civil and Political Rights is itself a pillar of international human rights law, and it has privacy protections, specifically under Article 17, banning arbitrary or illegal interference with privacy. This article has been central to making legality of mass surveillance measures more understandable by requiring any interference with privacy to be "prescribed by law" and to meet the test of proportionality and necessity. Article 8 of the ECHR further affords protection regarding respect for private life, home, and correspondence. But it does permit numerous exceptions, once more predominantly under rubrics of national security, where interference with privacy is done "in accordance with the law" and reasonable in a democratic society.

The different judicial constructions placed on the privacy right against surveillance rights center that there is the requirement of using a proportionality test in determining the balance that exists between individual freedom and state interest. In the UK, the case of R v. Secretary of State for the Home Department (2014) was a situation where the Investigatory Powers Tribunal considered the legality of bulk collection of data, and it was a trade-off between national security and privacy. The tribunal determined that the bulk collection of data was justifiable in certain circumstances

but required stronger safeguards and judicial oversight to prevent intrusions into the right of privacy of individuals.

Similarly, the Indian Supreme Court in Puttaswamy has also held that there could be a right to privacy which may only be limited where the limitation was necessary and proportionate. The Court reiterated once again that laws of surveillance had to remain under strict judicial supervision so as not to get transformed into arbitrary and excessive state intrusiveness.

Socio-Legal Implications of Emerging Surveillance Technologies

Mass surveillance technologies like facial recognition, AI, and biometric tracking, which have recently emerged, bring new privacy and personal freedom issues. These technologies can potentially allow governments and corporations to spy on humans like never before and without their knowledge or consent[17].

Facial recognition technology has long been in conflict with law enforcement agencies. Its use has been banned by San Francisco and other cities in the United States due to concerns regarding mass surveillance and racial profiling[18]. Similarly, facial recognition technology has been used by the government of China to trace and monitor communities, particularly the Uighur Muslims in Xinjiang, to raise human rights abuses concerns.

Socio-legal consequences of such technologies are profound and profound. On the one hand, they can assist governments in strengthening national security by enabling them to identify criminals and potentially stop terrorist operations, but on the other hand, such technologies create tremendous privacy concerns as they can be utilized for the round-the-clock surveillance of common citizens without their knowledge or against their right to anonymity and freedom from state interference. The situation gets worse because the individuals do not know what happens to their information, how it is collected, stored, or used due to the lack of transparency, monitoring, and accountability mechanisms.

Moreover, surveillance technologies pose a threat to the deepening of social inequalities since they have a propensity to disproportionately target marginalized groups. Thus, scholars like Ruha

[17] *Daniel J. Solove, Understanding Privacy* 1–3 (Harvard Univ. Press 2008).

[18] Kate Conger, Richard Fausset & Serge F. Kovaleski, San Francisco Bans Facial Recognition Technology, *N.Y. Times* (May 14, 2019)

Benjamin, in Race After Technology, express concerns about how surveillance technologies might feed racial biases and intensify already existing social fractures.

Suggestions for Balancing Surveillance and Privacy Rights

Balancing surveillance and privacy rights in the digital age is a great challenge. Such balance can be achieved through various reforms, which include legal reforms, improved oversight, and international cooperation. Some of the main suggestions to balance these two are as follows:

Transparency in Legal Frameworks

The laws for countries should ensure that surveillance is not an intrusion into the right to individual privacy. There is a need to have defined provisions on the kind of surveillance and reasons the government would engage in it and the extent it should be taken to. Laws, therefore, have to be grounded on necessity, proportionality, and legality for the appropriate surveillance measures to ensure that the limits are not reached in a wide scope or invading individual privacy. Additionally, citizens should receive information about surveillance through public disclosures and transparency reports to ensure accountability.

Eradication of Abuses through Strengthened Oversight Mechanisms

Independent oversight may be better achieved through the establishment of effective oversight over abuse of surveillance powers. This can be realized through the creation of independent bodies with regulatory functions or judicial review mechanisms over surveillance programs and legal standards. These bodies are obligated to carry out an investigation and audit over surveillance practices so that they are challenged or stopped to engage in illegal or disproportionate activities. Besides, review of surveillance laws should be mandated periodically to cope with new technology and the nature of emerging threats, in which surveillance measures will not go beyond what is reasonably necessary for national security.

International Cooperation on Data Protection

Where the digital data is global, international cooperation on standards is essential. Common data protection frameworks should be developed by countries to ensure the protection of privacy rights without compromising security concerns. This would involve lining up national law instruments with international instruments, such as the GDPR, creating the mechanism that will ensure cross border-data sharing across borders respecting principles of privacy and data protection. International bodies such as the United Nations or Council of Europe can push for both global standards and binding agreements that would regulate data transfer and secure people's rights even in national security threats.

With these steps in place, states can ensure citizens' rights to privacy and, at the same time, deliver security required for national defense and public safety.

Conclusion

In conclusion, findings on how conflicts between the issues of national security and privacy have a very complicated story to tell where surveillance meant to ensure public safety often tends to conflict with the very foundation of an individual's right of privacy. Case law analysis, statutes, and international conventions reflect that although the state does have a rightly defined interest in its defense, there is a proportionate need to balance this against personal freedoms such as the right to privacy. Pursued judicial interpretations of this nature - such as ACLU v. Clapper (U.S.) and Justice K.S. Puttaswamy v. Union of India (India) - substantially place emphasis on all the measures so conducted having tests of necessity, proportionality, and legality, particularly with relation to the latter in the emerging technologies with all the dark implications for privacy if regulation fails to hold good.

The key finding from this research is that although surveillance may be necessary in some circumstances to protect national security, it must always be conducted with a clear legal basis and in a manner that respects individual rights. Transparent legal frameworks, strong oversight mechanisms, and international cooperation on data protection are essential to ensure that privacy rights are not eroded by unchecked surveillance practices. The first focus will be on jurisprudential safeguards strong enough to preclude abuse but which also ensure redress for citizens.

In terms of the balance between national security and privacy, this is not just a legal challenge but an ethical one. Government and legal structures as well as internet or any related entities must ensure such surveillance is both ethical and legally sound. This involves safeguarding civil liberties while at the same time addressing the security needs of society. As the world continues to get smaller, it is essential that surveillance practices are constantly brought under scrutiny, and updated legal frameworks are adopted to keep pace with technological advancements. Only through a conscientious effort to balance these interests can we uphold both security and privacy in the modern era.