BALANCING NATIONAL SECURITY AND PRIVACY: THE LEGALITY OF MASS SURVEILLANCE IN INDIA, THE UK, AND THE USA

Manika Dass, Law College of Dehradun (Uttaranchal University)

ABSTRACT

Through a comparative legal examination of mass surveillance frameworks in India, the United Kingdom (UK), and the United States of America (USA), this article examines the complicated relation between individual privacy and national security. Governments claim that surveillance activities are necessary for dealing with cyber threats, terrorism, and other national security issues in an increasingly digitalized world. However, these initiatives frequently give rise to worries regarding the degradation of civil liberties, abuse of authority, and violation of the right to private. This article looks at the legal frameworks that govern mass surveillance in the three countries, emphasizing important pieces of legislation including the Foreign Intelligence Surveillance Act of the USA, the Investigatory Powers Act of the UK, and the Information Technology Act of India. It also analyzes landmark court rulings, such as Carpenter v. United States, Big Brother Watch v. United Kingdom, and K.S. Puttaswamy v. Union of India, to evaluate how courts have interpreted surveillance powers in relation to constitutional safeguards. The study makes the case that India's fragmented and secretive system lacks enough protections and accountability, whereas the United States and the United Kingdom have comparatively structured institutions with differing levels of judicial and parliamentary scrutiny. The study emphasizes the necessity of open, rights-based surveillance regulations that are necessary, proportionate, and subject to independent monitoring via this comparative lens. Legal systems must change in order to safeguard democratic values as new technologies like artificial intelligence and predictive analytics transform surveillance capacities. In order to guarantee a fair and legal surveillance system, the study ends with suggestions for balancing security requirements with privacy rights.

Introduction

In the current era, technology plays a vital role in governance and surveillance on the daily basis, even though mass surveillance is essential for national security but still it is a controversial tool. There has been several concerns regarding the privacy of the citizens and the governments around the world are justifying numerous surveillance programs which are required for preventing cyber threats, terrorism and other security risks. One of the biggest challenges in the modern times is to maintain a balance between national security and individual privacy.

The term mass surveillance means a complex of an entire or a large fraction of population in order to monitor a group of citizens.[1]India, United Kingdom, United States of America and other countries have implemented several surveillance programs like India's Central Monitoring System (CMS), UK's Investigatory Powers Act, and USA's PRISM program. These programs play a vital role in gathering intelligence but also have faced criticism for the violation of fundamental rights.

It is important to balance national security and privacy in order to safeguard the democratic value and prevent misuse of power by authorities. While on one hand surveillance is important to prevent crime and terrorism and on the other hand, excessive monitoring can result in infringement of a person's freedom and harm public trust. There are legal frameworks in each country to regulate mass surveillance, but due to various controversies there is a need for accountability and transparency.

Under this article, we will examine the legality of mass surveillance in India, the UK and the USA in order to explore legal and constitutional protections to safeguard the privacy of each country. We will also examine whether the existing laws can efficiently maintain balance between national security and individual privacy of the citizens of their country.

Legal Framework for Mass Surveillance

With a defined legal framework for mass surveillance one can determine how government use, store and collect data to ensure the protection of individual rights. With the rapid

[1]https://www.privacyinternational.org/press-release/52/new-privacy-international-report-shows-21-european-countries-are-unlawfully

technological advancement and also increasing security threats, the countries have enacted laws to permit surveillance for public order, national security and crime prevention. Even though national laws provide guidelines for the operation of mass surveillance but they must also coordinate with international human rights obligations which make privacy a fundamental right. We will try to examine how these legal frameworks maintain a balance between national security and privacy.

India

The Indian legal framework for mass surveillance is fragmented; there is no definite statue that governs mass surveillance. There are various modern as well as colonial era laws that provide for the monitoring and interception of communication for the interest of national security, public order, and internal security. Even though there are numerous concerns regarding privacy, but still judicial control and transparency regarding surveillance are limited.

The Indian Telegraph Act, 1885

The foremost law governing the telephone surveillance is Indian Telephone Act, 1885, the *section 5(2)* of which permits the state or central government to intercept communications "in case of any emergency or public safety" in the interest of sovereignty and integrity of India, national security, or public order.[2]The Supreme Court's landmark judgment *People's Union for Civil Liberties V. Union of India* (1997), which mandates that interceptions must be authorized by competent authority and reviewed by a committee.[3]

The Information Technology Act, 2000

As digital communication grows, the government can now intercept, monitor, or decrypt any information using a computer resource for the same purposes as the Telegraph Act[4] according to the Information Technology Act of 2000, particularly *Section 69*. Procedures for such interceptions are outlined in the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

[2]Indian Telegraph Act, 1885, Section 5(2)
[3]*People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301
[4] Information Technology Act, 2000, Section 69

However, the procedure mostly depends on executive discretion and lacks judicial monitoring.

The Central Monitoring System (CMS)

Without direct assistance from telecom service providers, government agencies can intercept phone conversations, emails, and internet activities in real time with the help of India's Central Monitoring System (CMS), which is run by the Centre for Development of Telematics (C-DOT)[5]. Despite being designed to simplify legal interception, the CMS's lack of statutory support and transparency create significant questions regarding accountability and possible misuse.

Other Surveillance Mechanisms

India has also introduced other surveillance mechanisms such as:

- NATGRID (National Intelligence Grid): helps law enforcement and intelligence organizations by integrating information from various government databases.
- NETRA (Network Traffic Analysis): The Defense Research and Development Organization (DRDO) created it, to track keywords in internet traffic.

These systems raise ethical and legal concerns since they function under general administrative authorities and intelligence mandates without particular legislative permission.

USA

The United States has established a comprehensive legislative framework to regulate surveillance operations, particularly when it comes to counterterrorism and national security. Legislative acts, executive orders, and judicial oversight procedures are all part of the legal structure. These rules have changed to reflect the increasing hazards posed by the

[5] Government of India, Ministry of Communications, Lok Sabha Unstarred Question No. 668, answered on 5th December 2012

digital world, but they have also sparked serious concerns about privacy rights, especially in the wake of high-profile disclosures like those made by Edward Snowden in 2013.

Foreign Intelligence Surveillance Act (FISA), 1978

In order to create rules for the monitoring and gathering of foreign intelligence data between foreign powers and their operatives suspected of terrorism or treason within the United States, the Foreign Intelligence Surveillance Act (FISA) was passed. The Foreign Intelligence surveillance Court (FISC), established under FISA, is a secret court that grants requests for monitoring by federal organizations such as the National Security Agency (NSA)[6].

The government's capacity to carry out widespread surveillance was further increased by FISA amendments including the FISA Amendments Act of 2008 (FAA). The FAA's Section 702 permits the NSA to obtain, without a warrant, the electronic communications of foreign-based non-U.S. individuals, including, inadvertently, U.S. citizen data[7].

USA PATRIOT Act, 2001

The USA PATRIOT Act, which was passed in the wake of the 9/11 attacks, greatly expanded the scope of surveillance. Significant civil rights concerns were raised when *Section 215* of the Act allowed the mass collection of telecommunication metadata from U.S. residents, including call duration, numbers phoned, and time stamps.[8]

However, Section 215 expired in 2015 and was replaced by the USA FREEDOM Act in response to intense protest and judicial review. This Act limited the amount of data that could be collected in bulk and required that telecom firms keep data that could only be accessed by government agencies through specific requests that were authorized by the FISC.[9]

Executive Order 12333

Executive Order 12333, which was signed by President Ronald Reagan in 1981, describes

[6] Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801–1885
[7] FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436
[8] USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001)
[9] USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268

the functions and duties of the CIA and the NSA, among other U.S. intelligence organizations. It is frequently used to defend surveillance practices not covered by FISA or the PATRIOT Act[10] and allows the gathering of foreign intelligence data outside the United States. Critics contend that EO 12333 permits extensive and unrestricted surveillance capabilities because it functions mostly outside of judicial or congressional scrutiny.[11]

Constitutional Considerations

Privacy isn't specifically mentioned in the U.S. Constitution, but the Fourth Amendment shields people from "unreasonable searches and seizures." According to court interpretation, this includes some privacy protections, especially with regard to communications and tangible property. Nonetheless, the Fourth Amendment's relevance to digital monitoring is still a developing field of law.[12]

UK

One of the most detailed and well-organized surveillance laws in the democratic world is found in the United Kingdom. The UK government has created a legal framework that gives law enforcement and intelligence agencies extensive monitoring capabilities, motivated by national security concerns, particularly in the wake of terrorist threats. To protect civil liberties, these authorities are complemented by a number of oversight and accountability procedures.

Investigatory Powers Act 2016 (IPA)

The foundation of the UK's surveillance system is the Investigatory Powers Act 2016, sometimes known as the "Snooper's Charter." It created new surveillance powers with comprehensive legal procedures and revised and consolidated several earlier laws pertaining to surveillance, including the Regulation of Investigatory Powers Act 2000 (RIPA). In an effort to improve supervision and legitimacy, the Act also requires a "double-lock" system, whereby surveillance warrants need to be authorized by both a government minister and an impartial court.

[10] Executive Order 12333, 46 Fed. Reg. 59941 (Dec. 4, 1981)
[11] Human Rights Watch, “With Liberty to Monitor All,” July 2014
[12] U.S. Const. amend. IV; Katz v. United States, 389 U.S. 347 (1967)

Human Rights Protections

The Human Rights Act of 1998 reflects the UK's domestic legal duties as a signatory to the European Convention on Human Rights (ECHR). The right to respect for one's home, correspondence, and private and family life is guaranteed by *Article 8* of the ECHR. As a result, any invasion of privacy must be appropriate, required, and legal. The ECHR determined that parts of the UK's monitoring system were incompatible with the ECHR because they lacked adequate safeguards and oversight in cases like "Big Brother Watch and Others v. the United Kingdom."

National Intelligence Grid (NATGRID)

It raises questions about bulk data collecting since it tracks suspects in real time by integrating data from several databases and organizations.[13]

The challenges to civil freedoms are increased by the fact that, in contrast to many Western democracies, these programs function with little independent control and little public exposure.

Judicial Interpretation of Mass Surveillance

As courts try to strike a balance between national security concerns and fundamental rights like privacy, freedom of expression, and due process, the legitimacy of mass surveillance has come under more and more judicial scrutiny. The limits of legal surveillance are greatly influenced by judicial interpretation, particularly in democracies where the court is required to restrain the executive branch. Courts in the US, UK, and India have rendered significant rulings that are consistent with their own constitutional systems and legal traditions.

United Kingdom

The UK Supreme Court decided in *Privacy International v. Investigatory Powers Tribunal (IPT) (2019)*, one of the landmark cases, that the IPT's (which regulates surveillance) rulings

[13] NATGRID Project Overview, Ministry of Home Affairs

may be subject to judicial review[14]. In order to guarantee that intelligence services might be held responsible, this was an important step.

The European Court of Human Rights (ECHR) previously determined in *Big Brother Watch v. United Kingdom (2021)* that certain elements of the UK's bulk interception system infringed under the European Convention on Human Rights' (ECHR) Articles 8 (right to privacy) and 10 (freedom of expression)[15]. The Court determined that the UK's system lacked sufficient protections against misuse, especially with regard to confidential communications and journalist sources.

United States of America

The Second Circuit Court of Appeals' decision in *ACLU v. Clapper (2015)*, which declared that the National Security Agency's (NSA) mass collection of phone metadata under Section 215 of the PATRIOT Act, was unlawful[16]. The court raised significant privacy concerns and determined that such extensive data collection was not permitted by law.

The U.S. Supreme Court later decided in *Carpenter v. United States (2018)* that law enforcement organizations need a warrant in order to access past cell phone location data[17]. This signaled a change in court opinion, acknowledging that digital information should be strongly protected by the Fourth Amendment from arbitrary searches and seizures.

India

The Supreme Court ruled in People's Union for Civil Liberties (PUCL) v. Union of India (1997) that, without fair and reasonable procedures, telephone tapping violates the right to privacy guaranteed by Article 21 of the Constitution[18]. Procedural safeguards, such as Home Secretary approval and committee review on a regular basis, were ordered by the Court. It did not, however, establish judicial supervision.

[14]*Privacy International v. Investigatory Powers Tribunal* [2019] UKSC 22
[15]*Big Brother Watch and Others v. the United Kingdom*, ECHR (App no. 58170/13, 62322/14, and 24960/15), 2021
[16]*American Civil Liberties Union v. Clapper*, 785 F.3d 787 (2d Cir. 2015)
[17]*Carpenter v. United States*, 138 S. Ct. 2206 (2018)
[18]*PUCL v. Union of India*, (1997) 1 SCC 301

The K.S. Puttaswamy v. Union of India (2017) decision, in which a nine-judge panel unanimously affirmed the right to privacy as a basic right under the Constitution[19], marked a dramatic change. The Court decided that any privacy restriction must pass the proportionality, necessity, and legality standards. This ruling has had a significant influence on future interpretations of surveillance laws, urging a balance between individual rights and state objectives, even if it is not specifically related to monitoring.

In Manohar Lal Sharma v. Union of India (2021), the Supreme Court affirmed that governmental surveillance must be within the law and subject to judicial oversight by appointing an independent technical committee to look into the Pegasus spyware claims[20].

Privacy vs. National Security: Key Debates

The conflict between privacy and national security has emerged as one of the most crucial and intricate legal and moral dilemmas of our digital age. While civil rights activists caution that such measures frequently come at the expense of fundamental liberties, governments contend that heightened surveillance is necessary to stop organized crime, terrorism, and cyber dangers. Finding a balance that protects personal privacy without sacrificing public safety is the difficult part.

The Necessity vs. Proportionality Dilemma

Whether monitoring methods are appropriate and essential is one of the main topics of discussion. A common tenet of national security organizations is that extensive surveillance is necessary for anticipatory threat identification. Nonetheless, privacy advocates and judges contend that measures need to be specifically designed. In Big Brother Watch v. UK, the European Court of Human Rights ruled that the right to privacy was breached by mass interception without protections.[21]

Lack of Transparency and Oversight

Many surveillance operations, according to critics, operate in secret with little judicial or legislative oversight. For instance, the Central Monitoring System in India conducts

[19]*Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1
[20]M*anohar Lal Sharma v. Union of India*, Supreme Court of India, W.P. (Crl.) No. 314/2021
[21]*Big Brother Watch v. United Kingdom*, ECHR (2021), App nos. 58170/13 and others

surveillance mostly without public awareness or judicial oversight.[22] Edward Snowden's exposes in the USA revealed the NSA's extensive data gathering, which many believed went beyond the law.[23]

National Security as a Justification for Abuse

The abuse of "national security" as a general defense that results in the monitoring of political opponents, journalists, and activists is another issue. The Pegasus spyware controversy raised concerns about unrestrained surveillance powers around the world by exposing how governments may target people without accountability.[24]

The Slippery Slope to a Surveillance State

There is a growing concern that, particularly in environments with an authoritarian biased, surveillance may have a chilling effect on free expression and protest once it becomes common. The UN High Commissioner for Human Rights has cautioned that a high level of surveillance risks civic space and democratic participation.[25]

Comparative Analysis

The ongoing battle to strike a compromise between individual privacy protection and national security is reflected in democratic nations' mass surveillance policies and procedures. Although the United States (USA), the United Kingdom (UK), and India all use surveillance for valid security reasons, there are notable differences in their legal systems, degrees of monitoring, and dedication to transparency. A comparative analysis provides insightful information about obstacles and best practices.

National Security as a Primary Justification:

National security, maintaining public order, and preventing crime or terrorism are some of the justifications used by all three nations to support monitoring. This emphasis is reflected

[22] Standing Committee on IT, Lok Sabha Report (2014)
[23] Barton Gellman et al., "Documents Reveal NSA Surveillance," *The Washington Post* (2013)
[24] Supreme Court of India, Pegasus Case, W.P. (Crl.) No. 314/2021
[25] UN Human Rights Council, "The Right to Privacy in the Digital Age," A/HRC/27/37 (2014)

in laws such as the UK's Investigatory Powers Act (2016), India's IT Act (2000), the USA's PATRIOT Act (2001), and FISA (1978).

Bulk Data Collection Capabilities:

Every nation has implemented legal framework or authorized agencies to conduct mass data collecting or monitoring. For example:

- India's Central Monitoring System (CMS)
- The UK's bulk interception regime under the Investigatory Powers Act
- The USA's NSA metadata collection, revealed by Edward Snowden

Privacy Concerns and Legal Challenges:

The lack of transparency and scope of surveillance operations led to opposition from courts, civil society, and privacy groups in all three nations.

Key Differences in Legal and Oversight Mechanisms

Aspect	**India**	**UK**	**USA**
Judicial Oversight	Minimal; mostly executive review	Present; Judicial Commissioners involved	FISC reviews certain surveillance; warrant requirements
Dedicated Surveillance Law	No (based on old colonial-era laws)	Yes (Investigatory Powers Act, 2016)	Yes (FISA, PATRIOT Act, USA FREEDOM Act)
Transparency Mechanisms	Absent	Moderate (reports and oversight reports published)	Improving; some disclosures post-Snowden
Constitutional Right to Privacy	Recognized in 2017 (Puttaswamy)	Via Human Rights Act (ECHR Article 8)	Through 4th Amendment jurisprudence

The Future of Mass Surveillance

The scope and complexity of mass surveillance keep changing as technology does. Government surveillance of populations is changing as a result of emerging technologies including artificial intelligence (AI), facial recognition, biometric tracking, and predictive analytics. These technologies create new ethical and legal issues by enabling unprecedented levels of real-time observation. The rise of big data, smart cities, and Internet of Things (IoT) devices expands the ways in which people can be watched.

As a result, nations are starting to reconsider and update their surveillance laws. The proposed AI Act and the EU's General Data Protection Regulation (GDPR) seek to control the use of surveillance technology, particularly in high-risk situations. Similarly, requests for strengthened digital privacy laws in the US have been impacted by legal discussions that followed Carpenter v. United States. Although it lacks strong safeguards against government surveillance, India's planned Digital Personal Data Protection Act (2023) is a move in the right direction.

The ability of legal institutions to adapt to new technologies will determine how widespread monitoring develops in the future. Transparent legislation, judicial supervision, data minimization, and independent regulatory agencies will all be necessary to strike a balance between individual privacy and national security. Without these protections, surveillance runs the risk of turning into a control mechanism rather than a defense. In the future, civil society representation and public awareness campaigns will be essential to ensuring that monitoring strengthens democracy rather than weakens it.

Conclusion

In conclusion, India, the UK, and the USA continue to face a difficult legal and moral dilemma when it comes to striking a balance between individual privacy and national security. Each nation takes a different approach: the UK functions under strict statutory constraints like the Investigatory Powers Act, while the USA places an emphasis on judicial monitoring through frameworks like FISA. However, India lacks a thorough legal system, which raises questions regarding unrestricted surveillance. Excessive or veiled surveillance can undermine civil liberties and democratic principles, even while national security is a valid state objective. To keep this balance, effective oversight, transparency, and judicial

accountability are essential. Modern, rights-based legal standards that protect privacy without sacrificing security are necessary given the rapidly changing digital context. In the end, a democratic society needs to make sure that surveillance systems are appropriate and legal in order to build public confidence and guard against abuse. To guarantee that privacy and national security coexist in a fair and just way, the legal systems in all three countries must keep evolving.

References

- Banisar, D. (2011). *National intelligence authorities and surveillance in the EU: A human rights perspective*. European Parliament. Retrieved from https://www.europarl.europa.eu
- Human Rights Watch. (2014). *Big Brother Comes to India: Government and Surveillance of the Internet and Telecommunications*. Retrieved from https://www.hrw.org
- Liberty UK. (2016). *A guide to the Investigatory Powers Act*. Retrieved from https://www.libertyhumanrights.org.uk
- Office of the United Nations High Commissioner for Human Rights (OHCHR). (2014). *The Right to Privacy in the Digital Age*. Retrieved from https://www.ohchr.org
- Supreme Court of India. (2017). *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
- UK Parliament. (2016). *Investigatory Powers Act 2016*. Retrieved from https://www.legislation.gov.uk
- United Nations. (1948). *Universal Declaration of Human Rights*. Retrieved from https://www.un.org/en/about-us/universal-declaration-of-human-rights
- U.S. Congress. (1978). *Foreign Intelligence Surveillance Act (FISA)*. Retrieved from https://www.law.cornell.edu
- U.S. Congress. (2001). *USA PATRIOT Act*. Retrieved from https://www.justice.gov/archive/ll/highlights.htm