ISSN: 2581-8651
Vol-8, Issue-2, Mar-Apr 2026
Peer-Reviewed Journal

Journal of Humanities and Education Development (JHED)

Survival of Right to Privacy under Administrative Surveillance: A Comparative Legal Study

Pawan Bindal[1], Dr. Ramveer Singh[2]

[1]Ph.D. Scholar, MVN University, Palwal, Haryana, India
[2]Associate Professor, MVN University, Palwal, Haryana, India

Keywords*— *Administrative Surveillance, Privacy, Right

Received: 05 Feb 2026;

Received in revised form: 03 Mar 2026;

Accepted: 08 Mar 2026,

Published on: 11 Mar 2026

***Abstract*—** *The right to privacy, recognised as a fundamental human right, faces serious challenges in the era of expanding administrative surveillance. Governments across the world increasingly rely on mass surveillance to address concerns of national security, crime prevention, and efficient governance. However, such practices often result in excessive data collection, intrusion into personal autonomy, and the risk of misuse of sensitive information. This paper examines the survival of privacy rights amid growing state surveillance, focusing on the delicate balance between individual freedoms and legitimate state interests. It analyses legal frameworks governing surveillance in democratic societies and evaluates the adequacy of existing privacy safeguards. Landmark judicial decisions, including K.S. Puttaswamy v. Union of India and Carpenter v. United States, are critically examined. The study also explores how technological advancements such as artificial intelligence, biometric systems, and data mining intensify privacy concerns. Emphasising proportionality and necessity, the paper advocates stronger oversight, transparency, and privacy-oriented digital governance to protect privacy rights.*

I. INTRODUCTION

The right to privacy is one of the most rudimentary and inherent elements of human dignity and sovereignty. The right to privacy has been debated exceedingly in the present digital age. With the fast-industrialized exponential growth of technology and an increased reliance on digital governance, administrative surveillance has gained importance as a significant issue. Governments worldwide justify surveillance measures as necessary for ensuring national security, law enforcement, and administrative efficiency. However, these measures often come at the expense of individual privacy, raising questions about the balance between state interests and fundamental rights. The conflict between privacy and surveillance has intensified with the rise of mass data collection, artificial intelligence-driven monitoring, and predictive analytics. This study explores the survival of the right to privacy under administrative surveillance, examining its legal foundations, challenges, and possible safeguards.

The rise in surveillance technologies has radically changed the contours of privacy rights. Traditionally, privacy has been considered an inalienable right that guards individuals from unrequired state incursion. However, the post-9/11 dispensation has seen a rapidly expanding state surveillance in the name of counterterrorism, crime prevention, and governance enhancement. Programs such as PRISM[1] in the United States, China's social credit system[2], and Aadhaar-based biometric identification in India[3] illustrate the growing breadth of administrative surveillance.

[1] Greenwald, G., & MacAskill, E. (2013, June 7). NSA Prism program taps into user data of Apple, Google and others. *The Guardian*. https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

[2] Creemers, R. (2018). China's social credit system: An evolving practice of control. *SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.3175792

[3] Unique Identification Authority of India. (n.d.). *Aadhaar*. https://uidai.gov.in/

This study's significance lies in its attempt to bridge the gap between legal protections and the realities of surveillance mechanisms. While governments argue that surveillance enhances national security and public safety, it can also lead to mass surveillance, data breaches, and the erosion of civil liberties. The study will critically analyze whether privacy can coexist with the growing demands of administrative surveillance by focusing on a balanced approach to ensure security without compromising fundamental rights.

1.1 Research objective

The primary objective of this research is to assess the survival of the right to privacy in the context of administrative surveillance. The study aims to:

A. Analyse the impact of administrative surveillance on privacy in democratic and authoritarian regimes.
B. Evaluate the effectiveness of existing legal frameworks in protecting privacy.

1.2 Research methodology and scope of study

This research adopts a multidisciplinary approach, integrating legal analysis, case study evaluation, and policy assessment. The methodology comprises two primary components:

1.2.1 Legal and Doctrinal Analysis**:** A thorough examination of constitutional provisions, statutory laws, and judicial interpretations forms the core of this study. Key legal documents, including the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), the European Convention on Human Rights (ECHR), and national constitutions, will be analysed. Special attention will be given to judicial precedents, particularly the rulings in K.S. Puttaswamy v. Union of India, Carpenter v. United States, and other landmark cases that have shaped privacy jurisprudence.

1.2.2 Comparative Case Study Approach**:** The study will compare administrative surveillance practices across different jurisdictions, including:

- United States: The role of the National Security Agency (NSA), the USA PATRIOT Act[4], and the Foreign Intelligence Surveillance Act (FISA)[5].
- European Union: GDPR's[6] impact on privacy and the European Court of Human Rights rulings on surveillance.
- India: The Aadhaar biometric database, its privacy implications, and Supreme Court judgments.

These case studies will provide a global perspective on the effectiveness and challenges of privacy protection in different legal and political frameworks.

The research is limited to analysing state-led surveillance rather than private-sector surveillance. However, it acknowledges the growing role of corporate entities in data collection and their collaboration with governments, which further complicates privacy concerns.

The research highlights the growing tensions between privacy and administrative surveillance. It underscores the significance of privacy as a fundamental right, the threats posed by expanding state surveillance, and the necessity for robust legal protections. The study aims to contribute to the legal and policy discourse by examining existing frameworks, identifying gaps, and proposing solutions to ensure the survival of privacy rights in an era of pervasive surveillance. Through a combination of legal analysis, case studies, and policy recommendations, this research aspires to provide a comprehensive understanding of how privacy can be preserved amid increasing state surveillance efforts.

II. WHAT IS PRIVACY?

The concept of the 'Privacy' is not new to us, it always is available to us. Only the form and jurisdiction of the 'Privacy' are changed. It starts with a 'Right to Live Alone' but now it deals with social, virtual, economic, and personal privacy. The right to privacy has evolved significantly over time, shaped by changes in societal values, legal interpretations, and technological advancements.

2.1 Privacy in Ancient and Early Societies

Early concepts of 'Privacy' can be traced back to ancient civilizations, though the term "privacy" as we understand it did not exist. In societies, privacy is available in the form of individual boundaries, personal respect, and honour. Norms and ethics of society show the decorum of privacy in life. In respect of social interest making things confidential and doing some daily activities under the curtail show the presence of privacy.

2.2 Privacy in Religious and Philosophical Thought (Medieval Period)

[4] (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).
[5] *Foreign Intelligence Surveillance Act of 1978*, 50 U.S.C. 1801–1885c (2023).
[6] General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, 2016 O.J. (L 119) 1.

During the medieval period, religious traditions such as Christianity, Judaism, and Islam, Hinduism introduced the idea of personal dignity and respect, indirectly supporting privacy by emphasizing the sanctity of family and home life. Rituals emphasized the importance of personal moral space, which laid an early foundation for the recognition of individual boundaries and autonomy.

2.3 Privacy and Individual Rights (Enlightenment and 18th Century)

The Enlightenment period: with its emphasis on individual rights and personal liberty, saw the emergence of privacy as a social and philosophical concept. Thinkers like John Locke discuss about privacy in his work "Two Treaties of Government" . In his work, he treated privacy as the output of natural law theory. Jean-Jacques Rousseau in 1762 in his book 'The Social Contract' promoted the idea that individuals have natural rights, including autonomy over their personal lives. This period also witnessed the rise of constitutional frameworks (e.g., the U.S. Constitution) that implicitly protected privacy through provisions safeguarding property and freedom from government intrusion.

2.4 'Privacy' as a Legal Right (19th Century)

The manifest recognition of 'Privacy' as a legal right occurred in the 19th century. In 1890, 'American lawyers Samuel Warren and Louis Brandeis' published the seminal paper "The Right to Privacy" in the Harvard Law Review. They contended that everyone should have the "right to be left alone" and highlighted the requirement for 'Privacy' protection against the press and emerging technologies like photography. This paper established the groundwork for privacy law in the 'United States' and inspired similar legal protections globally.

The law regarding trespass in the Indian Penal Code somehow shows the protection of 'Privacy' in respect of property and chattels. Not only that laws regarding religion and defamation also protect personal and emotional privacy.

The provision of privileged communication between legal counsel and client in the Indian Evidence Act, of 1872 also shows the presence of privacy.

Apart from these concepts privacy in consideration and privacy of parties in the Indian Contract Act, also resemble the right to privacy.

And, in family law, only the concerned aggrieved party can file a case against each other also a concept of privacy of a family.

2.5 Privacy in the Age of Communication (20th Century)

The 20th century marked the expansion of privacy rights as new technologies such as the telephone, radio, and television enabled greater public access to private information. The legal is going to adopt this right.

- The Universal Declaration of Human Rights (1948) by the United-Nations, she recognized privacy in Article 12, establishing a global standard for privacy rights.
- Article 17 of the "International Covenant on Civil and Political-Rights (ICCPR)" emphasizes the protection of the 'Privacy' for citizens in each country.
- The United Nations International Convention on the Protection of the Rights of All Migrant Workers and members of their families also declared the eight of privacy for migrants.
- Article 21 of the Indian Constitution by manifestation of the right to life with dignity ensures the 'right to-privacy' of a citizen of India.
- After the case of Kharak Singh vs. State Of Uttar Pradesh and Ors . In the case of Gobind vs. State of M.P. and in the case of PUCL vs. Union of India the Supreme Court confirm the 'Privacy' under the umbrella of the "Right to Life". The court held that to live a dignified law in a civilized society it is necessary to ensure the right to privacy.

2.6 'Privacy' in the Digital-Era (Late 20th and Early 21st Century)

The late 20th century witnessed the rise of the digital-age with computers, the internet, and mobile communication, reshaping privacy concerns. Personal data became an asset, and the capacity to collect, store, and process information grew exponentially.

The case of K.S. Puttaswamy (Retd.) vs. Union of India plays a vital role in the recognition and evolution of the 'Privacy'. In this case court confirms the 'Privacy' with citizens of India as a fundamental right and makes the government accountable for its protection. It is the first time the court concerned about virtual privacy. Court male comment on data protection, virtual privacy, unethical surveillance, and biometric information.

2.7 Privacy in the Age of Surveillance and Big Data (Present Day)

Today, privacy is challenged by pervasive data collection, artificial intelligence, and surveillance technologies. The widespread use of social media, location tracking, and biometric data collection has heightened concerns over how personal data is used and protected.

With that view, India comes with The Digital Personal Data Protection Act (DPDPA),2023 . The DPDPA

mandates that data fiduciaries obtain explicit-consent from individuals before collecting, processing, or sharing their data. It emphasizes transparency, accountability, and the rights of individuals, including the right to access, correct, and erase personal data. The Act also establishes a Data Protection Board to oversee compliance and address grievances. By aligning with global standards, the DPDPA seeks to enhance user trust and safeguard privacy in an increasingly data-driven world.

In this way, the evolution of privacy reflects society's ongoing effort to balance individual freedom with technological progress. As the boundaries of personal information and privacy become increasingly blurred, understanding the historical context of privacy is essential for shaping future policies and practices that respect both individual rights and collective security in the digital-age.

Table-1 *Evolution of of privacy*

ANCIENT PERIOD	In the ancient periods privacy came under the criteria of individual boundary, family respect, norms, human, dignity, and ethics.
MEDIEVAL PERIOD	In this period religious and philosophical aspects of society emphasized individual rights and personal liberty.
EARLY MODERN PERIOD	In this period international organizations started to recognize the 'Privacy' and unethical surveillance.
MODERN PERIOD	In the modern digital world right to privacy includes virtual privacy, stalking, data security, digital surveillance, etc.

Privacy is a fundamental human right that involves the ability of individuals to control their personal information, autonomy, and space. It enables people to decide what information they wish to share or keep private, thus fostering personal freedom, dignity, and individuality. Privacy is not limited to physical spaces but extends to digital spaces and informational privacy, particularly relevant in the modern information age. The term Privacy has been defined by so many scholars in some of the defined below-

Table-2 Scholar's contribution in definition of privacy

1	**Alan Westin (1967):**	"Privacy is the claim of individuals to determine for themselves when, how, and to what extent information about them is communicated to others"[7].
2	**Ruth Gavison (1980):**	"Privacy is a condition where one is protected from unwanted access by others, ensuring autonomy and freedom"[8].
3	**Daniel Solove (2006):**	"Privacy is not a single concept but a family of related problems involving control over personal information and protection from intrusion"[9].
4	**Hyman Gross (1967):**	"Privacy involves the ability to control what others know about you and to limit their access to your personal life."[10]
5	**Fried Charles (1970):**	"Privacy is rooted in the respect for persons and is essential for intimacy and relationships."[11]
6	**Judith DeCew (1997):**	"Privacy encompasses informational, accessibility, and decisional control dimensions."[12]
7	**Anita Allen (1988):**	"Privacy is crucial for self-development and maintaining personal dignity."[13]
8	**Julie Inness (1992):**	"Privacy is based on the idea of respect for personal boundaries and control over intimate decisions."[14]
9	**Adam Moore (2003):**	"Privacy involves a realm where individuals can make personal decisions free from interference."[15]
10	**Beate Roessler (2005):**	"Privacy ensures personal space for self-expression and development of autonomy."[16]

In last it can be concluded that the right to privacy is completely related to personality. Everyone has a different personality with himself for example one personality with friends, one personality at the workplace, and one

[7] Westin, A. (1967). *Privacy and freedom*. Atheneum.

[8] Gavison, R. (1980). Privacy and the limits of law. *Yale Law Journal, 89*(3), 421–471. https://doi.org/10.2307/795891

[9] Solove, D. J. (2006). *The digital person: Technology and privacy in the information age*. New York University Press.

[10] Gross, H. (1967). *The concept of privacy*. Anchor Books.

[11] Fried, C. (1970). *An anatomy of values: Problems in the philosophy of law*. Harvard University Press.

[12] DeCew, J. (1997). *In pursuit of privacy: Law, ethics, and the rise of technology*. Cornell University Press.

[13] Allen, A. (1988). *Privacy: Philosophical dimensions of the law*. Oxford University Press.

[14] Inness, J. (1992). *Privacy: A tradition in crisis*. Oxford University Press.

[15] Moore, A. (2003). *Privacy rights: Moral and legal foundations*. University of Pennsylvania Press.

[16] Roessler, B. (2005). *The value of privacy*. Cambridge University Press.

personality with the spouse, one personality with family members, etc. And the right to privacy ensures the right to secure and maintain this personality. It means under the right to privacy, no person can't know about another personality of an individual without his consent.

In this way **"Right to privacy can be defined as no person shall know about another's personal information without his consent except according to procedure established by law"**.

2.8 Significance of privacy

'Privacy' is recognized as a fundamental essential right after a long struggle. Now 'Privacy' is treated as the right to life (Article 21)[17]. The right to protect personality is one of the major requirements for a dignified life. If we don't allow the 'Privacy', then it becomes hard to enhance the personality of an individual. And improvement in the personality is the essence of life. The 'Privacy' plays a significant role in leading of good life. Everyone should be free in discretion to showcase himself. To know about someone should be done with his consent. It's not about the invasion of the right to information, it's about the protection of the right to a dignified life. The significance of the right of privacy is defined below-

1. Protection of Individual Dignity: Individuals can manage their data and make decisions about their lives without undue intervention thanks to privacy, which protects their autonomy and dignity.
2. Freedom of Speech and Expression (Article 19)[18]: Privacy creates an atmosphere in which people feel free to voice their ideas, opinions, and convictions. It safeguards the privacy of communications, which is necessary in a democracy.
3. Personal Autonomy: People can make choices about their bodies, relationships, and personal lives thanks to their right to privacy, which encourages self-determination and individual liberty.
4. Prevention of Abuse: Privacy protects against abuses of power and overreach by the government. By limiting monitoring and control, it shields people from capricious official actions and rights abuses.
5. Promotion of Trust: Intimacy and trust are fostered by privacy in interpersonal relationships and social interactions. People can exchange knowledge without worrying about being taken advantage of or judged because of it.
6. Discrimination Prevention: Privacy can shield people from prejudice based on traits, inclinations, or situations. It gives underrepresented groups a safe place to express who they are.
7. Innovation Facilitation: A strong right to privacy promotes innovation by giving people and companies the assurance they need to experiment with new services and technology without worrying about illegal data exploitation.
8. Maintenance of secrecy: In several professional domains, including healthcare, law, and finance, where maintaining secrecy is critical to preserving client and professional confidence, privacy is vital.
9. Data Protection: The privacy is becoming more closely associated with 'data protection in the digital age'. It guarantees that people oversee how their personal information is gathered, used, and disseminated.
10. Legal Framework and Accountability: By acknowledging the 'Privacy' , a legal framework is established that makes institutions and governments responsible for privacy violations, encouraging openness and accountability.

In this way, it can be concluded that the right to privacy is significantly required for the enforcement of the right to life. In a democratic civilized society, it requires that everyone should have some personal space where they can do their activities.

III. ADMINISTRATIVE SURVEILLANCE: JURISDICTION AND SCOPE

3.1 Understanding Administrative Surveillance

Administrative surveillance is the systematic collection of information by state agencies for security, governance, and regulation. It is not judicial or law enforcement surveillance, which needs probable cause or warrants. Administrative surveillance is mainly undertaken for policy implementation, national security, and the efficiency of public services. It encompasses the digital collection of data, CCTV surveillance, biometric verification, monitoring of the internet, and mass data analysis.

3.2 Justifications for Government Surveillance

The rationale for surveillance by the government is based on several legal, security, and administrative justifications. Governments defend surveillance on the following assumptions:

[17] Constitution of India, 1950
[18] Constitution of India, 1950

National Safety and Security: One of the most fundamental motivations for administrative monitoring is preventing terrorism, cybercrime, and other national security threats. Governments contend that immediate information gathering and monitoring have the potential to prevent possible dangers from occurring before they become actual threats. The USA PATRIOT Act[19], which was passed following the 9/11 attacks, illustrates how the surveillance statutes are broadened during periods of crisis to strengthen intelligence collection.

Crime Prevention and Law Enforcement Assistance: Surveillance helps law enforcement officials to identify and catch criminals. Automated facial recognition technology, traffic monitoring, and communication interception are regularly cited as indispensable means of upholding law and order. The Indian Telegraph Act, of 1885[20], offers legal support for government interception of electronic communication in certain circumstances.

Regulatory Governance and Compliance: Surveillance is imperative to ascertain tax compliance, financial regulations, immigration policy, and health-related compliance. It is regarded as pivotal to public administration's effectiveness in enforcing compliance. The Aadhaar Act, 2016, of India[21], requiring biometric authentication for public services, is a perfect example of regulatory surveillance.

Public Health and Emergency Response: Governments employ surveillance to monitor disease outbreaks, follow pandemic conditions, and enforce public health interventions. This was particularly evident during the COVID-19 pandemic, where digital surveillance was utilized in contact tracing and vaccine administration. The Epidemic Diseases Act, of 1897[22], provided authorities with sweeping powers to observe and regulate health emergencies.

Economic and Infrastructural Development: Digital governance and smart city initiatives depend on administrative surveillance to streamline public services like traffic control, energy efficiency, and waste management. Surveillance for urban planning is typically justified under municipal governance statutes and environmental protection statutes.

[19] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).
[20] The Indian Telegraph Act, 1885, No. 13, Acts of Parliament, 1885 (India).
[21] Government of India. (2016). *The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016*. https://www.indiacode.nic.in
[22] Government of India. (1897). The Epidemic Diseases Act, 1897. Ministry of Health and Family Welfare.

3.3 Impact of Mass Surveillance on Civil Liberties

Although administrative surveillance has several advantages, it also sparks important issues around the right to privacy and other civil rights. The consequences of mass surveillance are:

- Erosion of Privacy Rights: Large-scale collection of data, usually done in the absence of explicit consent, results in degradation of the privacy rights of individuals. The government's capacity to monitor people's movements, calls, and digital activities can contribute to a high degree of personal loss of autonomy. The Indian Supreme Court, in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)[23], established that privacy is a constitutional right under Article 21 of the Indian Constitution[24], limiting state surveillance.
- Chilling Effect on Free Speech and Expression: Mass surveillance makes individuals hesitant to express opposing viewpoints, become politically active, or stage protests for fear of being targeted by the government and facing the consequences. The European Court of Human Rights in Big Brother Watch v. United Kingdom (2021)[25] held that mass surveillance schemes need to be subject to rigorous legal supervision to ensure protection against free expression rights violations.
- Risk of Abuse and Overreach: Lacking robust legal frameworks and control mechanisms, administrative monitoring can be used politically, for biased targeting, or improper sharing of data with non-governmental institutions. The U.S. Foreign Intelligence Surveillance Act (FISA)[26] has been faulted for being overly broad in scope and opaque in operation.
- Disproportionate Targeting of Minority Communities: Disproportionate targeting of racial, religious, and ethnic communities by surveillance technologies has been criticized on grounds of inducing systemic biases and discrimination. Predictive policing technology has been contested in various jurisdictions based on perpetuating racial profiling.
- Legal and Ethical Challenges: Artificial intelligence and predictive analytics in surveillance raise issues of algorithmic bias, data security, and the likelihood of wrongful incrimination. The Indian Supreme Court has noted that laws governing surveillance should agree with

[23] *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
[24] Government of India. (1950). *Constitution of India, Article 21*.
[25] European Court of Human Rights. (2021). *Big Brother Watch v. United Kingdom*, App. Nos. 58170/13, 62322/14, 24960/15.
[26] U.S. Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 (1978)

the doctrines of proportionality and necessity so as not to be excessive.

IV. NATIONAL AND INTERNATIONAL LEGAL FRAMEWORKS GOVERNING SURVEILLANCE AND PRIVACY

4.1 National Legal Frameworks

All developed and developing country faces a clash between privacy and administrative surveillance. There is a lot of legal measures have been made to counter this problem:-

Table -3 Legal Framework for Administrative Surveillance

1	**India**	Constitutional Protection (Article 21 and Puttaswamy Judgment) The right to privacy was declared a fundamental right under Article 21 of the Indian Constitution in the case Justice K.S. Puttaswamy v. Union of India (2017)[27]. The Supreme Court stressed that privacy is an integral part of the right to life and personal liberty. The Information Technology Act, 2000: The Information Technology Act, 2000 (IT Act)[28] forms the legal basis for electronic surveillance in India. Section 69 of the Act authorizes the government to intercept, monitor, and decrypt information in the national interest of sovereignty, security, and public order. There are, however, apprehensions regarding judicial oversight and transparency. The Indian Telegraph Act, 1885: Section 5(2) of the Indian Telegraph Act[29], 1885 gives the government the right to intercept messages in times of public emergencies or in the cause of public safety. The Rules under the Telegraph Act also provide further details on the interception process, including issues of concern over executive discretion being too high. The Personal Data Protection act, 2023: India's Digital Personal Data Protection Act, 2023[30], modelled after the EU General Data Protection Regulation (GDPR)[31], aims to control data gathering and processing. Nevertheless, the bill gives wide-ranging exemptions to the government to use personal data for surveillance activities, fuelling concerns about unbridled state surveillance.
2	**United States**	The Fourth Amendment the Fourth Amendment to the U.S. Constitution[32] protects citizens against unreasonable searches and seizures, requiring a judicial warrant based on probable cause. The Foreign Intelligence Surveillance Act (FISA), 1978[33]: FISA establishes procedures for the surveillance of foreign powers and agents. It created the Foreign Intelligence Surveillance Court (FISC), which oversees warrant applications for electronic surveillance. The USA PATRIOT Act, 2001: The USA PATRIOT Act[34] widened the surveillance capacity of the government after the 9/11 attacks, and it provided for bulk data gathering and the notorious Section 215 program, under which mass phone metadata surveillance was authorized. The CLOUD Act, 2018: The Clarifying Lawful Overseas Use of Data (CLOUD) Act[35] makes it easier for law enforcement to access data across borders by allowing authorities to seek electronic data from companies, even if abroad.
3	**European**	General Data Protection Regulation (GDPR), 2018: The GDPR[36] imposes

[27] *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
[28] Government of India. (2000). *The Information Technology Act, 2000* (No. 21 of 2000).
[29] The Indian Telegraph Act, 1885, No. 13, Acts of Parliament, 1885 (India).
[30] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
[31] General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, 2016 O.J. (L 119) 1
[32] (U.S. Const. amend. IV)
[33] *Foreign Intelligence Surveillance Act of 1978*, 50 U.S.C. §§ 1801–1885c (2023).
[34](USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).
[35] Clarifying Lawful Overseas Use of Data (CLOUD) Act, Pub. L. No. 115-141, § 105, 132 Stat. 1213 (2018).
[36] General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 April 2016 on the protection of

	Union	strict data collection, processing, and transfer rules, with a guarantee that personal data will be dealt with openly and lawfully. The European Convention on Human Rights (ECHR)[37]: Article 8 of the ECHR ensures the right to private and family life if such is subject to lawful and proportionate limitations. The e-Privacy Directive, 2002[38]: The directive complements the GDPR in that it safeguards confidentiality in electronic communications and puts a stop to unauthorized data monitoring.
4	**United Kingdom**	The Investigatory Powers Act, 2016 (IPA)[39]:- The IPA, otherwise referred to as the "Snooper's Charter," provides UK authorities with sweeping surveillance powers, including bulk data collection. The European Court of Human Rights (ECtHR) has declared aspects of this legislation incompatible with the right to privacy.

4.2 International Legal Mechanisms

Some international legal tools attempt to govern state surveillance and uphold privacy protection:-

Table-4 International mechanism for Administrative Surveillance Regulation

1	**The International Covenant on Civil and Political Rights (ICCPR), 1966**	Article 17 of the ICCPR[40] promises protection against arbitrary interference with privacy. The United Nations Human Rights Committee has reaffirmed that surveillance programs should be necessary, proportionate, and under independent review.
2	**The Universal Declaration of Human Rights (UDHR), 1948**	Article 12 of the UDHR[41] provides that no one shall be subjected to arbitrary interference with his privacy, home, or correspondence. Though not legally binding, it has helped influence international norms.
3	**The Convention on Cybercrime (Budapest Convention), 2001**	The treaty, crafted by the Council of Europe[42], sets international cooperation about investigations of cybercrime and ensures guarantees for privacy.
4	**United Nations Guidelines**	The United Nations Guidelines for the Regulation of Computerized Personal Data Files, 1990[43]:- These rules set data protection standards that involve data collection restrictions, transparency, and accountability.
5	**OECD Guidelines**	The OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data, 1980[44]:- The Organisation for Economic Co-operation and Development (OECD) published guidelines encouraging equitable practices in data processing and limiting the unjustified invasion of privacy.

The legal regimes for surveillance and privacy manifest the constant tension between security needs and human rights. While universal instruments promote privacy guarantees, national legislation tends to give states carte blanche for surveillance. Strong oversight, judicial checks,

natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, 2016 O.J. (L 119) 1

[37] European Convention on Human Rights, Nov. 4, 1950, 213 U.N.T.S. 221.

[38] uropean Parliament and Council. (2002). *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (e-Privacy Directive)*. Official Journal of the European Communities, L 201, 37–47. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32002L0058

[39] Investigatory Powers Act 2016, c. 25. https://www.legislation.gov.uk/ukpga/2016/25/enacted

[40] International Covenant on Civil and Political Rights, art. 17, Dec. 16, 1966, 999 U.N.T.S. 171.

[41] United Nations. (1948). *Universal Declaration of Human Rights*, Article 12. https://www.un.org/en/about-us/universal-declaration-of-human-rights

[42] Council of Europe. (2001). *Convention on Cybercrime* (ETS No. 185). https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[43] United Nations. (1990). *Guidelines for the regulation of computerized personal data files*. Retrieved from https://www.un.org

[44] Organisation for Economic Co-operation and Development (OECD). (1980). *OECD guidelines on the protection of privacy and transborder flows of personal data.* OECD. https://www.oecd.org/digital/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data.htm

and powerful data protection laws are vital in ensuring that the right to privacy endures amidst the tide of administrative surveillance.

V. JUDICIAL INTERVENTION ON PRIVACY AND ADMINISTRATIVE SURVEILLANCE

Administrative surveillance is a two-edged sword. While it has important governance and security roles, it also brings serious risks to civil liberties, especially the right to privacy. The legitimacy of surveillance practices is contingent on sound legal frameworks, open policies, and strong mechanisms of oversight, which weigh against national security needs and safeguard core rights. Thus, it is necessary to create surveillance legislation that is proportionate, indispensable, and in keeping with democratic values to safeguard the existence of the right to privacy during the era of administrative surveillance. Judicial precedent, constitutional safeguards, and international human rights standards have to be used for informing and implementing policies of administrative surveillance to maintain the precarious balance between security and liberty.

Table-5 Case Laws Administrative Surveillance and privacy

1.	**United State**	Katz v. United States (1967)[45] – Held that the Fourth Amendment guarantees individuals, not locations, a reasonable expectation of privacy. Smith v. Maryland (1979)[46]– Established the third-party doctrine, holding that information voluntarily given to third parties is not protected by the Fourth Amendment. Carpenter v. United States (2018)[47]– Called for a warrant for law enforcement to obtain historical cell-site location information (CSLI). American Civil Liberties Union v. Clapper (2015)[48]– Held that the NSA's bulk telephone metadata collection was unlawful under the Patriot Act. United States v. Jones (2012)[49]– Held that affixing a GPS tracker to a suspect's vehicle was a search under the Fourth Amendment. Riley v. California (2014)[50]– Held that police must have a warrant to search a suspect's cell phone when arrested.
2.	**European court**	Zakharov v. Russia (2015)[51]– Held that Russia's mass surveillance scheme did not contain proper safeguards, contravening Article 8 of ECHR. Klass v. Germany (1978)[52]– Affirmed state surveillance measures but stressed the importance of enforcing strict legal controls to avoid abuses. Weber and Saravia v. Germany (2006)[53]– Accepted that mass surveillance needs to be proportionate and subject to independent supervision. S. and Marper v. United Kingdom (2008)[54]– Found holding DNA samples of innocent people breached the right to privacy. Malone v. United Kingdom (1984)[55]– Held that the UK's telephone tapping activities contravened Article 8 of European Convention on Human Rights (ECHR). Big Brother Watch v. United Kingdom (2021)[56]– ECHR held UK's mass surveillance legislation breached rights to privacy.
3.	**United Kingdom**	R (Privacy International) v. Investigatory Powers Tribunal (2019)[57]– Held that judicial review of the UK's Investigatory Powers Tribunal is applicable. Campbell v. Mirror Group Newspapers (2004)[58]– Held public figures too had a right against media intrusion of privacy.

[45] *Katz v. United States*, 389 U.S. 347 (1967).
[46] *Smith v. Maryland*, 442 U.S. 735 (1979).
[47] Carpenter v. United States, 585 U.S. ___ (2018).
[48] *American Civil Liberties Union v. Clapper*, 785 F.3d 787 (2d Cir. 2015).
[49] *United States v. Jones*, 565 U.S. 400 (2012).
[50] *Riley v. California*, 573 U.S. 373 (2014).
[51] *Zakharov v. Russia*, App. No. 47143/06, ECHR (2015).
[52] *Klass v. Germany*, 2 E.H.R.R. 214 (1978).
[53] *Weber and Saravia v. Germany*, App No. 54934/00, 2006-XI Eur. Ct. H.R.
[54] *S. and Marper v. United Kingdom*, 2008 ECHR 1581.
[55] Malone v. United Kingdom, 7 E.H.R.R. 14 (1984).
[56] *Big Brother Watch v. United Kingdom*, App. Nos. 58170/13, 62322/14 & 24960/15, ECLI:CE:ECHR:2021:0525JUD005817013 (Eur. Ct. H.R., May 25, 2021).
[57] R (Privacy International) v. Investigatory Powers Tribunal, [2019] UKSC 22.
[58] *Campbell v. Mirror Group Newspapers*, [2004] UKHL 22.

4.	**Canada**	R v. Spencer (2014)[59]– Found police need a warrant to access subscriber details associated with an IP address. Hunter v. Southam Inc. (1984)[60]– Held that the Canadian Charter of Rights and Freedoms guards against unreasonable searches. R v. Duarte (1990)[61]– Held that private conversations must be judicially authorized prior to being intercepted by the police.
5.	**Australia**	Dow Jones & Co Inc v. Gutnick (Australia, 2002)[62]– Dealt with jurisdictional privacy matters in the context of online defamation and data privacy.
6.	**Ireland**	Max Schrems v. Data Protection Commissioner (Ireland, 2015)[63]– resulted in the annulment of the EU-U.S. Safe Harbor Agreement for cross-border data transfers because of privacy issues.
7.	**South Africa**	Minister of Safety and Security v. X (South Africa, 2012)[64]– Held that surveillance and data gathering must be proportionate and legally justified.
8.	**India**	K.S. Puttaswamy v. Union of India (2017) (Privacy Judgment)[65]– A classic case in which the Supreme Court of India in a unanimous verdict established privacy as a fundamental right under Article 21 of the Constitution. Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar Case) (2018)[66]– The court established the constitutional validity of Aadhaar but put curbs on its use to ensure privacy. PUCL v. Union of India (1997) (Telephone Tapping Case)[67]– Laid down parameters for lawful interception of communications to avoid misuse of surveillance power. Shreya Singhal v. Union of India (2015)[68]– Declared Section 66A of the IT Act as unconstitutional, holding that it was an infringement on free speech and privacy rights. Gobind v. State of Madhya Pradesh (1975)[69] – Engraved privacy as an unarticulated right within the right to life and liberty (Article 21). R. Rajagopal v. State of Tamil Nadu (1994) (Auto Shankar Case)[70] – Held the right to privacy as including safeguards against both state and private incursions. People's Union for Democratic Rights v. Union of India (1982)[71] – Enunciated guidelines to avert misuse of the state over the privacy of individuals. Selvi v. State of Karnataka (2010)[72] – Declared narco-analysis and polygraph tests as illegal on an insistence basis, safeguarding privacy in criminal investigations. Anuradha Bhasin v. Union of India (2020)[73] – Held that unplanned shutdowns of the internet are violations of basic rights, reiterating privacy online.

VI. CONCLUSION

The research on the survival of privacy under administrative surveillance highlights the fine line between individual rights and state security interests. The legal debate over privacy has significantly changed in national and international courts, reflecting a growing international

[59] R v. Spencer, [2014] 2 S.C.R. 212 (Can.).
[60] *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145 (Can.).
[61] *R v. Duarte*, [1990] 1 S.C.R. 30 (Can.).
[62] Dow Jones & Co Inc v. Gutnick, (2002) HCA 56, 210 CLR 575 (Austl.).
[63] Max Schrems v. Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650 (Court of Justice of the European Union, Oct. 6, 2015).
[64] *Minister of Safety and Security v. X*, (2012) (S. Afr.).
[65] *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
[66] Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar Case), (2018) 1 SCC 809.
[67] Public Union for Civil Liberties v. Union of India, (1997) 1 SCC 301 (India).
[68] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
[69] *Gobind v. State of Madhya Pradesh*, (1975) 2 SCC 148 (India).
[70] R. Rajagopal v. State of Tamil Nadu, AIR 1995 SC 264
[71] People's Union for Democratic Rights v. Union of India (1982)
[72] Selvi v. State of Karnataka (2010)
[73] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.

acknowledgment of the right to privacy as a core human right. Administrative surveillance continues to be a controversial topic where governments have used national security, law enforcement, and public interest as reasons to justify far-reaching data gathering and monitoring. We need to make a harmonious relation in both of them and adopt a protective approach. Individual security and individual sovergenity is not contradictory to each other. These are co-related to each other. To secure this issue following points can be used:-

- Privacy is a Constitutional or Human Right – Landmark judgments like K.S. Puttaswamy v. Union of India (2017)[74] in India and Carpenter v. United States (2018)[75] in the U.S. reaffirm that privacy is not a privilege but a constitutional or human right in most jurisdictions. Courts have time and again held that privacy protection is available to digital domains, communications, and personal data.
- Surveillance Laws Tend to Lack Oversight – Numerous government surveillance schemes, including the U.S. NSA's PRISM program and Russia's SORM system, has been criticized for functioning with minimal transparency and judicial supervision. The ECHR's decision in Zakharov v. Russia (2015)[76] serves to illustrate the dangers of mass surveillance absent adequate safeguards. It is the duty of all state that whenever they make any policy for surveillance keep the space of survival of right to privacy.
- Judicial Interpretation Adapts with Technology – Courts across the globe have recognized the challenges presented by contemporary technology. The transition from Katz v. United States (1967)[77] to Carpenter v. United States (2018)[78] in the United States illustrates how the judiciary is evolving legal doctrines to safeguard privacy in the digital era. Judiciary have to understand its duty and keep vigilant on the right to privacy.
- Governments Rationalize Spying on Security Reasons – National security is the most widespread reason for administrative surveillance. Laws passed after 9/11, such as the Patriot Act in the U.S. and India's IT Rules, 2021, reflect that governments frequently use threats to security as the reason for broadening their powers of surveillance. But, on the name of security you cannot diminish the soverginity of individual. All surveillance data should be collected with bonafide intention with minimal use.
- Data Privacy Laws Are Imperative to Privacy – Legal instruments like the EU General Data Protection Regulation (GDPR) and India's Digital Personal Data Protection Act (DPDPA), 2023, reflect an increasing international focus on data privacy. In this digital era we require to secure the virtual identity of person.
- Judicial Review Plays a Crucial Role – Cases such as Privacy International v. Investigatory Powers Tribunal (2019)[79] in the UK show that judicial bodies remain essential safeguards against excessive surveillance. Courts have a key role in ensuring proportionality and necessity in government surveillance programs.

The right to privacy is a pillar of democracy, individual autonomy, and liberty. Administrative surveillance, though in some situations necessary, must be made transparent, accountable, and proportionate to avoid undermining fundamental rights. Courts and legislatures across the globe must be ever watchful in protecting privacy from unbridled government surveillance so that technological advancement does not happen at the expense of individual freedom.

REFERENCES

[1] Indian Penal Code, 1860.
[2] Indian Telegraph Act, 1885.
[3] Information Technology Act, 2000.
[4] The Aadhaar Act, 2016.
[5] The Digital Personal Data Protection Act, 2023.
[6] Fourth Amendment to the U.S. Constitution.
[7] Foreign Intelligence Surveillance Act (FISA), 1978.
[8] USA PATRIOT Act, 2001.
[9] CLOUD Act, 2018.
[10] General Data Protection Regulation (GDPR), Regulation (EU) 2016/679.
[11] European Convention on Human Rights (ECHR), Article 8.
[12] e-Privacy Directive, 2002.
[13] Investigatory Powers Act, 2016.
[14] Universal Declaration of Human Rights (UDHR), 1948, Article 12.
[15] International Covenant on Civil and Political Rights (ICCPR), 1966, Article 17.
[16] Convention on Cybercrime (Budapest Convention), 2001.
[17] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980.
[18] United Nations Guidelines for the Regulation of Computerized Personal Data Files, 1990.
[19] Allen, A. L. (1988). Uneasy access: Privacy for women in a free society. Rowman & Littlefield.

[74] *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1
[75] Carpenter v. United States, 585 U.S. (2018).
[76] *Zakharov v. Russia*, App. No. 47143/06, ECHR (2015).
[77] *Katz v. United States*, 389 U.S. 347 (1967).
[78] Carpenter v. United States, 585 U.S. (2018).
[79] R (Privacy International) v. Investigatory Powers Tribunal, [2019] UKSC 22.

[20] DeCew, J. (1997). In pursuit of privacy: Law, ethics, and the rise of technology. Cornell University Press.
[21] Fried, C. (1970). An anatomy of values: Problems of personal and social choice. Harvard University Press.
[22] Gross, H. (1967). The concept of privacy. New York University Law Review, 42, 34–52.
[23] Inness, J. (1992). Privacy, intimacy, and isolation. Oxford University Press.
[24] Moore, A. (2003). Privacy rights: Moral and legal foundations. Penn State University Press.
[25] Richards, N. (2015). Intellectual privacy: Rethinking civil liberties in the digital age. Oxford University Press.
[26] Roessler, B. (2005). The value of privacy. Polity Press.
[27] Solove, D. J. (2006). A taxonomy of privacy. University of Pennsylvania Law Review, 154(3), 477–564.
[28] Solove, D. J. (2008). Understanding privacy. Harvard University Press.
[29] Rachels, J. (1975). Why privacy is important. Philosophy & Public Affairs, 4(4), 323–333.
[30] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[31] PUCL v. Union of India, (1997) 1 SCC 301.
[32] Shreya Singhal v. Union of India, (2015) 5 SCC 1.
[33] Gobind v. State of Madhya Pradesh, (1975) 2 SCC 148.
[34] R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.
[35] Selvi v. State of Karnataka, (2010) 7 SCC 263.
[36] Anuradha Bhasin v. Union of India, (2020) SCC Online SC 25.
[37] Olmstead v. United States, 277 U.S. 438 (1928).
[38] Katz v. United States, 389 U.S. 347 (1967).
[39] Smith v. Maryland, 442 U.S. 735 (1979).
[40] Carpenter v. United States, 585 U.S. ___ (2018).
[41] United States v. Jones, 565 U.S. 400 (2012).
[42] Riley v. California, 573 U.S. 373 (2014).
[43] United Kingdom & European Court of Human Rights (ECHR)
[44] Big Brother Watch v. United Kingdom, App. Nos. 58170/13, 62322/14, 24960/15 (ECHR, 2021).
[45] Campbell v. Mirror Group Newspapers, [2004] UKHL 22.
[46] Malone v. United Kingdom, App. No. 8693/79 (ECHR, 1984).
[47] Zakharov v. Russia, App. No. 47143/06 (ECHR, 2015).
[48] Klass v. Germany, App. No. 5029/71 (ECHR, 1978).
[49] S. and Marper v. United Kingdom, App. Nos. 30562/04, 30566/04 (ECHR, 2008).
[50] Weber and Saravia v. Germany, App. No. 54934/00 (ECHR, 2006).
[51] R v. Spencer, [2014] 2 S.C.R. 212.
[52] Hunter v. Southam Inc., [1984] 2 S.C.R. 145.
[53] R v. Duarte, [1990] 1 S.C.R. 30.
[54] Dow Jones & Co Inc v. Gutnick, [2002] HCA 56.
[55] Max Schrems v. Data Protection Commissioner, (2015) C-362/14.
[56] Minister of Safety and Security v. X, (2012) ZACC 27.
[57] Human Rights Watch. (2014). With liberty to monitor all: How large-scale US surveillance is harming journalism, law, and American democracy.
[58] United Nations Human Rights Council. (2014). The right to privacy in the digital age.
[59] Snowden, E. (2019). Permanent record. Metropolitan Books.
[60] Amnesty International. (2019). Surveillance giants: How the business model of Google and Facebook threatens human rights.
[61] Electronic Frontier Foundation. (2021). Mass surveillance and privacy rights: A global review.
[62] Shoshana Zuboff (2019) – The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs.
[63] Bruce Schneier (2015) – Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. Norton.
[64] Paul Bernal (2018) – Privacy and Surveillance: Legal, Ethical and Social Aspects. Routledge.
[65] Neil M. Richards (2013) – The Dangers of Surveillance. Harvard Law Review, 126, 1934–1965.