SURVEILLANCE, PRIVACY, AND THE LAW: AN INDIAN PERSPECTIVE WITH COMPARATIVE INSIGHTS

Priyam Sharma[*]

ABSTRACT

The surveillance technologies of the modern age (such as CCTV cameras, biometric identification, artificial intelligence, and predictive analytics) are rapidly expanding both in the governmental and the non-governmental spheres, giving serious concerns regarding safeguarding the rights of privacy. The problem in democratic societies is how to balance the national security requirements and the individual liberties. This essay is a critical paper on legal implications of surveillance technologies with special reference to India, but provides the comparative insights of the United States and the European Union. It is a historical track of constitutional acknowledgment of privacy in Justice K.S. Puttaswamy v. Union of India and assesses main statutory frameworks, such as the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and the Telecommunications Act, 2023. The analysis highlights persistent gaps such as weak oversight, executive dominance, and broad national security exemptions. The paper wraps up by highlighting that unified surveillance legislation is urgently required to provide proportionality, accountability and safeguard of fundamental rights.

Keywords: Surveillance technologies, privacy rights, data protection, human rights.

[*] Assistant Professor, Law Department, Savitribai Phule Pune University

INTRODUCTION

Across various jurisdictions surveillance technologies now dominate every aspect of public and private spaces during modern times. These surveillance technologies combine biometric identification systems with GPS tracking and CCTV networks and social media monitoring capabilities alongside AI-based facial recognition systems to deliver national security and law enforcement capabilities as well as commercial advances. Their rapid spread has sparked serious worries about privacy destruction that created complex legal, ethical and constitutional challenges.[1]

National security requirements face an ongoing struggle with private space rights which proves both persistent and difficult to solve. After the 9/11 attacks counterterrorism measures quickened the development of surveillance systems while undermining the protection of procedural rights and constitutional due process. Digital surveillance has grown extensively during the COVID-19 pandemic to enable states along with corporations to track personal actions, locations and digital communications more thoroughly. The world's rapid adoption of contact tracing apps alongside facial temperature scanners and biometric-based movement controls demonstrates how surveillance practices that previously needed constitutional approval can now be normalized as standard practices. India's highest court recognized the right to privacy as fundamental through its landmark decision Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1. v. The Supreme Court established a tripartite examination of propriety in Union of India, (2017) 10 SCC 1 that combines legal justifications with necessity and proportionality. Through the Indian constitution the endorsement has situated privacy rights as part of a wider framework that includes Articles 14, 19, and 21. Practical execution of this right encounters significant difficulties stemming from regulations that fall short of addressing this need combined with executive agencies' invasive behavior and insufficient independent regulatory oversight. [2]

The General Data Protection Regulation from the European Union stands as an international standard which requires consent together with data minimization principles and clear accountability requirements. Surveillance programs in the United States exist as a mixture of

[1] Solove, Daniel J., "A Taxonomy of Privacy" (2006) 154(3) *University of Pennsylvania Law Review* 477
[2] David Lyon, *Surveillance After Snowden* (Polity Press, Cambridge, 2015)

Foreign Intelligence Surveillance Act (FISA) law and Fourth Amendment judicial decisions that determine how state interests align with privacy rights. Surveillance programs conducted by Five Eyes intelligence groups create complex legal issues regarding how law applies outside national boundaries and problems with protecting privacy rights of international citizens and monitoring cross-border data transfers.[3]

DEFINING PRIVACY IN LAW AND PHILOSOPHY

The diverse nature of privacy consists of independent dimensions which protect personal autonomy through honoring dignity and managing personal information access. The idea of privacy in philosophical terms defines each person's authority to create an unobstructed space around themselves in accordance with liberal democratic rules concerning individual self-expression and physical boundaries.[4] The legal dimension express privacy through different formulations that include: The right to be let alone emerged first in 1890 from Warren and Brandeis's work and later evolved into fundamental informational control and personal decision-making power in critical intimate issues (e.g., reproductive choices and sexual practices).

Justice K.S. Puttaswamy (Retd.) v. Union of India, 2017 10 SCC 1, a decision of the Supreme Court in India established the right to privacy. v. The Supreme Court of India in Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 identified privacy as an essential component of both Article 21's life and personal liberty provisions. The Court made clear that privacy functions as different intertwined rights instead of a single entity made up of bodily privacy alongside informational privacy and decisional autonomy. These legal tests for invasions were established to match international privacy standards in the court's decision. The European Court of Human Rights (ECtHR) expanded Article 8 of the European Convention on Human Rights (ECHR) to embrace personal data together with family life and home privacy and correspondence rights (S. and Marper v. United Kingdom, App. Nos. 30562/04 and 30566/04). United Kingdom, App. Nos. 30562/04 and 30566/04). American citizens receive

[3] International Principles on the Application of Human Rights to Communications Surveillance (Necessary and Proportionate Principles), July 2013
[4] Benjamin J. Goold, "Surveillance and the Political Value of Privacy" (2009) 1(2) *Amsterdam L. Forum* 3

Fourth Amendment protection against “unreasonable searches and seizures” which serves as the constitutional foundation for privacy during state surveillance operations.[5]

UNDERSTANDING SURVEILLANCE

Surveillance in its French language origin of surveiller (to watch over) encompasses the process of monitoring individuals or groups together with their information collection and data evaluation. Three main surveillance types exist: state surveillance through law enforcement and intelligence agencies and corporate surveillance managed by private organizations seeking profit alongside social surveillance conducted by digital peers. The legal scholarly analysis of surveillance often points to its ability to create a "chilling effect" for both speech freedoms and human conduct (Klayman v. Obama, 957 F.Supp.2d 1 (D.D.C. 2013)). Obama, 957 F.Supp.2d 1 (D.D.C. 2013))[6]. The Panopticon metaphor developed by Michel Foucault illustrates how disciplinary societies require internalizing conformity because of surveillance[7]. Modern surveillance operates through numerous decentralized community networks that support systems like algorithmic policing and facial recognition databases and real-time tracking methods. Surveillance methods restrict personal rights while remaining unclear to citizens and they distribute unequal impact based on racial and religious and caste-based criteria.

THE CONVERGENCE OF PRIVACY AND SURVEILLANCE IN LAW

The surveillance-versus-privacy conflict emerges from recognizing the state's responsibilities to protect public security and protect its residents' personal liberties. Surveillance authorization laws from governments rely on statements that protect national interest or public order and terrorism prevention. Unregulated surveillance laws create problems because they allow unchecked mass surveillance operations outside proper judicial and parliamentary oversight systems. Programs such as India's CMS and the U.S. PRISM have drawn widespread criticism because they operate without clear transparency measures which challenges their legal framework and proper scale of management. The lack of a uniform data protection law in India leads to fragmented privacy regulation while privacy protections respond only after particular

[5] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[6] Liberty and Others v. The United Kingdom, App. No. 58243/00, ECtHR (2018).
[7] Larry Klayman v. Barack Obama, 957 F. Supp. 2d 1 (D.D.C. 2013).

situations develop. Under the Digital Personal Data Protection Act, 2023 the government was granted exceptions to access personal data yet this regulatory exemption weakens the privacy protections established in Puttaswamy[8]. Public awareness regarding surveillance soared worldwide after Edward Snowden provided classified intelligence about mass data surveillance to the public in 2013. Mass telephone and internet data surveillance revealed by the National Security Agency (NSA) drove multiple jurisdictions to create new legal standards protecting privacy rights. International human rights obligations fell victim to the extent of surveillance capabilities which operated beyond territorial boundaries during the aftermath.[9]

NORMATIVE JUSTIFICATIONS AND CHALLENGES

The supporters of surveillance claim that today, nations face challenges such as transnational terrorism, pandemics, and cybercrime; hence, there is no option than to adopt surveillance systems. It is useful in curbing crime, protection of borders and during calamities. However, there is a normative argument necessary in justifying surveillance where the surveillance measures must meet four principles, namely legal requirement, lawful basis, reasonable suspicion, and necessity, compared to the proportionality of the crime. [10]Surveillance that is covert, arbitrary or unresponsive likewise fails these criteria and is constitutionally problematic. The core of the legal problem consists in defining the effective measures of control over personal data processing that would balance the protection of human rights with the state's legitimate interests. This includes legal sanctions, external and internal auditing, reporting that is required by the legislation, and procedures that allow for complaints by the public. Moreover, the question of surveillance cannot be fully deciphered without a special attention to private actors: data brokers, social media companies and other technologies companies that undertake surveillance with scarcely any legal restriction.[11]

[8] American Civil Liberties Union v. James Clapper, 785 F.3d 787 (2d Cir. 2015)
[9] United States v. Basaaly Moalin, 973 F.3d 977 (9th Cir. 2020).
[10] Carolyn Jewel v. National Security Agency, No. 4:08-cv-04373 (N.D. Cal. filed Sept. 18, 2008)
[11] Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295

LEGAL FRAMEWORKS GOVERNING SURVEILLANCE TECHNOLOGIES IN INDIA

Legal regulation of surveillance practices in India is weak, outdated, and quite discrete, as it consists of a rather complex system of legal acts. Despite the constitutionalism of privacy right in Justice K.S. Puttaswamy (Retd.) v. Supra, (2017) 10 SCC 1 India has not yet developed an all-embracing rights-based law regarding surveillance technologies and constitutional provisions. This section focuses on legal framework of surveillance in present India that involved basic legislative measures, executive arrangements and judicial administered efforts.[12]

STATUTORY PROVISIONS AUTHORIZING SURVEILLANCE

1. **The Indian Telegraph Act, 1885**:

   A post-colonial law of communication interception The Indian Telegraph Act, 1885, a colonial law, has long been used as the foundation of state powers of communication interception in India. In case of any emergency or when it was essential in regard to the safety of the population, sovereignty or public order, section 5(2) of the Act gave the government the authority of intercepting messages. Though the provision gave broad powers, it lacked elaborate measures to avoid abuse. Judicial intervention in People's Union for Civil Liberties (PUCL) v. Union of India (1997) tried to address these complaints by putting in place some procedural protection like the need to seek the authority of senior officials and to periodically examine the interception orders. The protections however were mostly executive in nature with little judicial checks and balances. Understanding that this old paradigm was insufficient in the digital age, parliament passed the Indian Telecommunications Act, 2023, which brings together and up-to-date telecommunication legislation. This Act clearly gives the repeal of the Telegraph Act, but also contains transitory provisions to maintain continuity of the necessary functions until the new structure is fully available. Therefore, although the Telegraph Act has been repealed by the law, certain of its provisions are temporarily still in operation and surveillance powers are still in place. This transitional solution highlights the continuity of colonial juridical after-

[12] The Indian Telegraph Act, 1885, § 5(2)

legacies as well as the difficulty of providing proportionality and responsibility in contemporary surveillance regulation[13].

Section 5 (2) of the Indian Telegraph Act 1885, is one of the oldest laws which was framed for the interception of telegram messages in case of emergent conditions or in the concerned of the communal security. Unfortunately, there is no detailed procedure outlined to protect the freedom and the independence of the judge to rule on these cases and it does not allow for any form of judicial supervision. In the PUCL v Union of India, (1997) 1 SCC 301 the supreme court has been given guidelines that the interception orders should be issued by the Home Secretary and these orders should be reviewed by an inter- departmental committee these are the executed safeguards rather than the judiciary safeguards.[14]

2. The Information Technology Act, 2000

According to IT Act 68 and 69B government has the authority to intercept, monitor or decrypt any information being generated/created, transmitted, received or stored in any computer resource if deemed necessary in the interest of security, maintenance of public order or prevention of incitement to offences. Rule 4 of the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, it was provided that directions can be issued by the designated officer. However, there is no room for pre-trial monitoring or post monitoring by the judiciary. The Act also does not address when, to what extent, or where data should be retained, minimized or even whether users asking for information should be notified of the consequences of their request.[15]

3. Other Sectoral Legislations and Surveillance Powers

Thus, the surveillance in India is not constrained to the intelligence and telecommunication laws only since many sectoral legislations throw their Effective powers of investigation and monitoring onto the state. Of them, the Unlawful Activities (Prevention) Act of 1967, the Indian Wireless Telegraphy Act of 1933, and the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act of 2016 directly affect the privacy of an

[13] Singh, R., *Telecom Act 2023: Promise and Pitfalls for Privacy*, Economic & Political Weekly, 2023
[14] Information Technology Act, 2000, § 69
[15] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

individual along with the kilometer of surveillance permitted to the state. Despite being adopted to achieve various goals to counter-terrorism, regulation of the use of wireless communication, and distribution of welfare all these legislations provide a complex legal framework that makes surveillance possible even without strict compliance to procedural requirements or pronounced judicial supervision.[16]

4. The Unlawful Activities (Prevention) Act, 1967

Formerly formulated to curb real and perceived threats to/fixed on the sovereignty and integrity of India, the UAPA has metamorphosed through the course of several amendments into the premier anti-terror law of the country. They can award widespread surveillance and interception of communication under the pretext of national security. Section 43D and 50 of the Kenyan constitution allow investigating agencies to search, seize or arrest without a warrant in cases of necessity. Furthermore, the terms "unlawful activity" and "terrorist act" have been left wide open to interpretation and have led to abuse and witch hunting. The National Investigation Agency (NIA) and other bodies that are designated can tap and investigate individuals and associations that are seen as suspicious and this is sometimes without clear accountability frameworks present. Explaining the chilling effect of the UAPA is the fact that the law lacks adequate checks, thus it is vulnerable to abuse, and politically motivated.[17]

5. The Indian Wireless Telegraphy Act, 1933

This legislation, which has its origin in the colonial period of the United States, regulates the possession of apparatus for wireless communication. Although it was created to regulate radio spectrum and prevent interferences, its consequent responsibilities have evolved include wiretapping of wireless communication. Section 3 – makes wireless telegraphy unlawful without a license and grants the authorities the power to seize any unlawful devices.[18]

Telecommunication Surveillance Act contains statutory recognition of the ability to monitor wireless communication with referenced in conjunction with the Telegraph Act and

[16] Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (Act 18 of 2016).
[17] The Unlawful Activities (Prevention) Act, 1967 (Act 37 of 1967)
[18] The Indian Wireless Telegraphy Act, 1933 (Act 17 of 1933)

Information Technology Act. Nevertheless, the given Act does not provide any mechanisms for judicial control or informing users about the process, thus marking state surveillance as uncontrolled and non-liquid. The complexity of the application of these principles is further seen in its application in the current digital and encrypted technologies.[19]

6. The Aadhaar Act, 2016

What was once sold as a welfare instrument that would enable targeted delivery of subsidies and services has turned into a colossal surveillance system. Section 33 of the Aadhaar Act allows sharing of identity information for the purpose of the security considerations on receipt of directions from an officer, not below the rank of the Joint Secretary. While the case is the most recent significant instalment of the Supreme Court's interpretation of the Right to Privacy, we need to jump back to September 2018 for a detailed discussion on the verdict, Justice K.S. Puttaswamy (Retd.). v. Union of India It comes as some relief that has placed some restrictions over the use of Aadhaar, yet there are looming issues about accumulation of biometric data; profiling, exclusion and leakage. Yet, there are many cases that show forced incorporation of Aadhaar into services based on self-enrollment and informed choice. The absence of a strong data protection law only adds to the concerns of state surveillance by way of Aadhaar linked databases.[20]

7. The Telecommunications Act, 2023:

The Telecommunications Act, 2023 is a massive effort to reform the archaic Indian telecom regulation regime by substituting the colonial style Indian Telegraph Act, 1885. The Act, which was enacted with the aim of harmonizing regulation with the fast changing communication technologies, brings together licensing, spectrum allocation, and security provisions in a single legal tool. Part of its most controversial parts includes the capabilities of surveillance and intercepting communications. The Act gives the government the authority to intercept, monitor or block telecommunication services under stipulated circumstances involving national security, order in the country or during emergencies. These powers are in paper supposed to be derived by the principles of necessity and

[19] Aadhaar (Authentication) Regulations, 2016, notified by the UIDAI under Notification No. 13012/64/2016/Legal/UIDAI dated 14 September 2016

[20] Aadhaar (Sharing of Information) Regulations, 2016, notified by the UIDAI under Notification No. 13012/64/2016/Legal/UIDAI dated 14 September 2016

proportionality, in agreement with the constitutional requirement of Justice K.S. Puttaswamy v. Union of India (2017). Nevertheless, critics believe that the Act offers wide exemptions in the name of national security, and gives the executive broad discretionary power, without subjecting the executive to intensive judicial scrutiny. This begs the question whether the proportionality test will be practically meaningfully applied. Researchers like Chaudhary (2024) and Singh (2023) argue that the Act is in fact an extension of an executive-oriented surveillance paradigm, where protections are in-house, not external. In contrast to systems adopted in some jurisdictions like the European Union that stipulate robust data protection authorities and judicial pre-authorization of surveillance, the Indian model depends on bureaucratic clearance. The Act may be an indication of the successful integration of legal provisions, but the surveillance provisions in the Act demonstrate a concept of continuity in the current practices. In the absence of clear checks and balances, independent regulatory, and judicial accountability, the equilibrium between state security and power and the individual right to privacy is fragile[21].

MASS SURVEILLANCE INFRASTRUCTURE

India has launched several mass surveillance program including,

1. **Central Monitoring System (CMS)** – Allows security agencies a direct footing into telecom traffic without having to visit individual service providers. Lack of parliamentary oversight and possible infringements of Article 21 has been castigated on CMS.
2. **NETRA- Network Traffic Analysis (NETRA)** – created by the Defence Research and Development Organization (DRDO), NETRA will track internet traffic for inputs related to suspicious activity. The algorithmic element sends alarm bells about false positives and discriminatory profiling.
3. **NATGRID (National Intelligence Grid)** – Connects the databases of several agencies (Scanner in transportation, such as railways, airlines, telecoms, public taxes, etc.) to assist in intelligence-sharing. It operates in a legal grey area devoid of a sweeping privacy or data protection law.
4. **Aadhaar Ecosystem** – Originally conceived for welfare identification, Aadhaar has been used for more and more authentication and surveillance applications. In Justice K.S.

[21] Singh, R., *Telecom Act 2023: Promise and Pitfalls for Privacy*, Economic & Political Weekly, 2023

Puttaswamy (Retd.) and Another v. Union of India and Others, (2019) 1 SCC 1 1 recognized its stature with limits, but its degree of mass profiling has been under contention.[22]

DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Although India passed the Digital Personal Data Protection (DPDP) Act, 2023 as a mechanism of regulating the processing of personal data, the provision of the Act is riddled with wide exceptions (such as the "State") especially under Section 17(2) which provides special dispensation to allow the processing of data without consent for the purposes of national security. The law is characterized by very little transparency or oversight on how surveillance is conducted as well as the absence of an independent data protection authority with adjudicatory powers.[23]

The DPDP Act also lacks:

a) Explicitly,
b) limits on surveillance, or interceptions.
c) Remedies to be presented to an individual following unlawful surveillance. Requirements on localization of the data or mechanisms of algorithmic accountability.

JUDICIAL RESPONSES AND LIMITATIONS

Indian courts have traditionally been obedient to the state when it comes to issues of national security. In PUCL v. Union of India and K.S. Puttaswamy, though the courts recognized privacy and identified the procedural norms, declined to take away the surveillance powers or impose parliamentary control. After the post Poothaswamy, very few judicial pronouncements have meaningfully responded to the surveillance capability of the state.

One among them stands out, namely the case of Pegasus spyware, which provides a clear example of the aforementioned form of cyberattack. In Manohar Lal Sharma v. Union of India, Crl. Writ Petition The 2021 No. 314 Supreme Court appointed a technical committee to inquire into complaints of unlawful surveillance[24]. The Court observed that national security cannot be

[22] Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others, (2019) 1 SCC 1
[23] The Digital Personal Data Protection Act, 2023 (Act 22 of 2023)
[24] *Manohar Lal Sharma v. Union of India*, Pegasus spyware case, (2021) SCC OnLine SC 985

used by the state to avoid judicial oversight at all. However, the final outcomes of the committee's findings are still confidential, and imply continued opacity.[25]

ABSENCE OF A UNIFIED SURVEILLANCE LAW

There is a growing consensus among scholars and civil society that India needs a dedicated, comprehensive law on surveillance which:

1. Regulates the parameters for the possibility of surveillance.
2. Establishes independent oversight bodies.
3. Permits judicial pre-authorization and periodic reviews.
4. Requires transparency reports and data subject rights.

The existing legal scene which has been established in different legislations and regulations lack to appeal up the constitutional and International human right standards. And it lacks accountability, and instead enshrines opaque and sprawling surveillance practices in the shell of executive authority.[26]

COMPARATIVE JURISPRUDENCE – MONITORING AND PRIVACY IN THE US, EU AND OTHER JURISDICTIONS.

A comparison of surveillance regimes in jurisdictions sheds light on global trends, the best practices and constitutional approaches to the right to privacy. The United States and the European Union are examples of powerful though conflicting models of regulation of surveillance technologies, while such countries as the United Kingdom, Canada and South Africa provide instructive hybrid frameworks. This part treats these regimes by describing both normative and procedural responses to the problems of digital spying.[27]

[25] Ministry of Electronics and Information Technology, Digital Personal Data Protection Bill, 2022
[26] Report of the Group of Experts on Privacy, Planning Commission of India (2012).
[27] National Security Agency Act of 1959, Pub. L. No. 86-36, 73 Stat. 63 (1959) (codified at 50 U.S.C. §§ 3601–3613)

1. United States: Constitutional rights and the power to conduct an expansive surveillance.

The Journal lacks the restriction imposed by laws on the use of such technologies; the regulation of the use of such devices in the United States is covered by the Fourth Amendment of the Constitution that stipulates that no person shall be subjected to "unreasonable searches and seizures". The jurisprudence has developed to consider surveillance issues via reasonable expectations of privacy, as expressed in Katz v. United States, 389 U.S. 347 (1967). The U.S. Supreme Court made privacy include electronic communications, but it remains a challenged area.[28]

a. Foreign Intelligence Surveillance Act (FISA), 1978

FISA creates the Foreign Intelligence Surveillance Court (FISC) that issues secret warrants of surveillance in relation to foreign threat. Besides, through the USA PATRIOT Act (2001) and the FISA Amendments Act (2008), particularly in the guise of Section 702, laws allowed the bulk collection of data without individual warrants. These have created controversies by their obscurity and reduced adversarial oversight.

b. National Security Agency (NSA) and PRISM Program

The 2013 Snowden disclosures revealed the extent of mass surveillance conducted by the NSA under the PRISM and Upstream programs. These revelations spurred legal reforms such as the USA FREEDOM Act (2015), which ended bulk telephony metadata collection by the NSA and required more transparency in FISC proceedings.[29]

c. Judicial Developments

In *Carpenter v. United States*, 138 S.Ct. 2206 (2018), the Supreme Court ruled that accessing historical cell phone location data without a warrant violates the Fourth Amendment, marking a significant shift in privacy jurisprudence. However, surveillance

[28] Katz v. United States, 389 U.S. 347 (1967)
[29] Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring (USA FREEDOM) Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 (2015) (codified in scattered sections of 18 and 50 U.S.C.)

under national security pretexts continues to operate with minimal public scrutiny or legislative resistance[30].

EUROPEAN UNION: DATA PROTECTION AND PROPORTIONALITY AS CORE PRINCIPLES

1. European Court of Human Rights (ECtHR) Jurisprudence

In *S. and Marper v. United Kingdom*, App. Nos. 30562/04 and 30566/04, the ECtHR held that indefinite retention of DNA and fingerprint data of unconvicted individuals violated Article 8 of the European Convention on Human Rights. The Court emphasized necessity and proportionality as central to evaluating state surveillance.

Similarly, in *Big Brother Watch and Others v. United Kingdom*, App. Nos. 58170/13, 62322/14, 24960/15 (2021), the ECtHR found UK's bulk interception regime to be in violation of privacy rights due to lack of adequate safeguards, even if carried out for legitimate aims like national security.[31]

2. Court of Justice of the European Union (CJEU) Decisions

In *Digital Rights Ireland Ltd v. Minister for Communications*, Joined Cases C-293/12 and C-594/12 (2014), the CJEU invalidated the Data Retention Directive, holding that indiscriminate data retention interferes with fundamental rights. The *Schrems I* and *Schrems II* decisions further invalidated transatlantic data transfer frameworks (Safe Harbor and Privacy Shield) due to concerns over U.S. surveillance practices.

3. General Data Protection Regulation (GDPR)

GDPR mandates strict conditions for data processing, including lawful basis, consent, and purpose limitation. It introduces Data Protection Impact Assessments (DPIAs), mandatory breach notifications, and enforcement through independent data protection authorities. While

[30] Chaudhary, A., *Privacy and Surveillance in India Post-DPDP Act*, Indian Law Review, 2024

[31] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified in scattered sections of 8, 12, 15, 18, 19, 21, 22, 28, 31, 42, 47, and 50 U.S.C.)

not directly a surveillance law, GDPR influences how both public and private surveillance technologies must operate in Europe.[32]

UNITED KINGDOM: HYBRID APPROACH WITH JUDICIAL OVERSIGHT

Post-Brexit, the UK has enacted the Investigatory Powers Act (IPA), 2016, also known as the "Snoopers' Charter." It codifies extensive surveillance powers, including:

a) Bulk data collection.
b) Equipment interference (state hacking).
c) Retention of internet connection records.

However, the IPA requires approval by both the Secretary of State and a Judicial Commissioner, introducing a “double lock” system. The Investigatory Powers Tribunal provides a forum for individuals to challenge unlawful surveillance. Despite these safeguards, the ECtHR has criticized UK surveillance for failing to provide effective redress and adequate oversight. Moreover, the IPA’s compatibility with post-Schrems II data transfer regimes remains under review.[33]

SOUTH AFRICA: CONSTITUTIONAL EMPHASIS ON DIGNITY AND OVERSIGHT GAPS

South Africa’s Constitution guarantees the right to privacy under Section 14. The Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA), 2002 governs surveillance. In *AmaBhungane Centre for Investigative Journalism NPC v. Minister of Justice*, 2021 (3) SA 246 (CC), the Constitutional Court held RICA unconstitutional for lacking safeguards such as post-surveillance notice and oversight independence. The ruling mandated judicial pre-authorization and robust accountability mechanisms, setting a strong precedent in the Global South. However, the challenge lies in implementing reforms amidst technological advancements and state resistance.[34]

[32] Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified as amended at 50 U.S.C. §§ 1801–1885c)
[33] Internet Freedom Foundation, 'Pegasus Project: Legal Briefing Paper', (2021)
[34] Carolyn Jewel v. National Security Agency, No. 4:08-cv-04373 (N.D. Cal. filed Sept. 18, 2008)

EMERGING SURVEILLANCE TECHNOLOGIES AND LEGAL CHALLENGES

Privacy violation and security concerns as new frontiers have been created by the arrival of emerging surveillance technologies. Although these technologies offer the prospects of a more secure nation and controlling crime, they entwine that nation's security with that nation's individual freedom in a confusing way. This section examines several of the latest surveillance technologies and their particular legal and ethical dilemmas.

1. Facial Recognition Technology (FRT)

The use of the facial recognition technology has been widely adopted and rapidly within the two sectors; which are private and the government. Utilized for identity verification, access control, police work, and mass surveillance, Privacy is a major concern in FRT as well as concerning FRT based discrimination.

a. Legal Issues

Consent and Intrusiveness: Unlike other forms of surveillance facial recognition tends to take place in public domains without explicit consent from persons. In places such as China, it is widely used for monitoring people in real-time, which directly threatens to undermine privacy rights. In India the police and other government bodies have used FRT without regulation and with little or no regulation concerning the need for consent or legal/rules protection[35].

Accuracy and Discrimination: Facial recognition systems are highly biased according to studies conducted along the lines of race, gender and age. This presents a huge legal problem on the aspect of equality and equal protection under the law. The uneven misidentification of the marginalized groups arouses concerns about possible violations of anti-discrimination laws and equal treatment guarantees.[36]

[35] Ramanathan, U., *From Telegraph to Telecom: Shifting Paradigms of Surveillance Law in India*, NUJS Law Review, 2024

[36] Electronic Frontier Foundation, 'Surveillance Self-Defense', (2022), available at https://ssd.eff.org/ (last visited May 7, 2025)

b. Legislative Developments

Several jurisdictions, such as the European Union and the United States, are enacting the use of restrictions on the use of facial recognition by government agencies and private entities. The GDPR issued by the EU ranks facial recognition as a form of biometric data which requires higher consent in terms of processing. On the other hand, India has not implemented any strong law that regulates the use of biometric surveillance.[37]

2. Drones and Unmanned Aerial Vehicles (UAVs)

Drones have emerged as a key tool in surveillance, particularly for border control, disaster management, and military operations. However, their growing use for civilian surveillance, including monitoring public protests or private citizens, has sparked privacy concerns.

Legal Issues

Intrusion into Private Spaces: Drones equipped with high-resolution cameras can easily trespass into private property or observe individuals in their homes, violating their right to privacy. This raises the question of where to draw the line between legitimate surveillance (e.g., for security purposes) and undue intrusion.

Lack of Regulation: In many countries, including India, the regulation of drones remains underdeveloped. The Civil Aviation Requirements (CAR) in India, issued by the Directorate General of Civil Aviation (DGCA), govern drone use but do not adequately address privacy concerns or impose restrictions on the use of drones by government agencies. The European Union has introduced the *European Union Drone Regulation*, which sets out clear guidelines for the use of drones, including restrictions on flying over private property without consent. In contrast, the US has proposed some state-level regulations, but a national framework remains lacking, creating a patchwork of laws that often fail to adequately protect privacy.[38]

INTERNATIONAL HUMAN RIGHTS LAW AND PRIVACY PROTECTION

[37] Neha Jain, 'Privacy and Proportionality in Surveillance Laws', (2022) 8(1) NLUJ L Rev 25
[38] European Union, General Data Protection Regulation (EU) 2016/679.

Deep seated in the world-wide discourse on surveillance is the right to privacy, as embodied in international human rights law. The UDHR and the ICCPR are the major foundational principles for the privacy protection and have considerable consequences for surveillance practices.

1. United Nations Universal Declaration of Human Rights (UN UDHR)

Article 12 of the UDHR provides that no one will be interfered with arbitrarily with regard to their privacy, family, home or correspondence. The UDHR therefore precedes the necessity to acknowledge privacy as an inherent human right that cannot be violated by state mechanisms such as surveillance. Its application area is narrowed down to state conduct, and does not apply directly to corporate or private sector surveillance[39].

2. International Covenant on Civil and Political Rights (ICCPR)

Article 17 of the ICCPR stipulating that individuals shall not be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence is one of the provisions that regulates surveillance. The United Nations Human Rights Committee (HRC) has, in interpreting this article, expanded it to cover various intelligence activities such as monitoring of communications and collection of personal data. Significantly, the HRC also indicates that any interference should be lawful, inevitable, and appropriate which are the principle of necessity and proportionality that guide privacy protections in national jurisdictions.[40]

3. Regional Human Rights Instruments

Even the ECHR, which are regional human rights instruments, provide considerable protections. Article 8 of the ECHR legitimately assures the right to respect for private and family life, home, and correspondence as well as for similar state interference, but only under certain and limited conditions (national security, or crime prevention, etc.). The European Court of Human Rights (ECtHR) has been especially important in maximizing the effect of

[39] Riley v. California, 573 U.S. 373 (2014)
[40] International Covenant on Civil and Political Rights, 1966, Art. 17

surveillance provisions, the release of binding jurisprudence on the surveillance practices of member States.[41]

4. The part played by United Nations and the specialized agencies.

The United Nations (UN) is having a lobby for privacy rights especially in surveillance. Although the UN has failed to promulgate such a regulating treaty on surveillance, its numerous organs have promulgated guidelines and reports that inform national policy and international norms.

5. The UN Resolutions on Privacy in General Assembly.

In 2013 the UN General Assembly unanimously approved a historic resolution stating that privacy is a universal human right in the information age. Resolution 68/167 clearly states that right to privacy includes safeguards against unlawful surveillance especially from the state actors. This resolution, while non-binding, puts a message across to states on how their obligations under international law in relation to human rights corporately require them to protect people from invasive surveillance practices.[42]

KEY FINDINGS

1. The Effect of Surveillance Technologies of Privacy on a Global Scale.

There are now pervasive surveillance devices, like facial recognition, predictive policing AI, drones, and biometric collection, to name just a few, for state and private use alike. Though these technologies promise improved security and efficiency, these also bring enormous privacy concerns. They make it possible to gather data without the explicit consent of people, to such an extent that one's privacy and autonomy can be violated.[43]

[41] Investigatory Powers Act, 2016 (UK)
[42] Paul M. Schwartz, 'Privacy and Democracy in Cyberspace', (1999) 52 Vand L Rev 1609
[43] *European Convention on Human Rights* (ECHR), Art. 8, Council of Europe, 1950

2. Legal Gaps and Inconsistent Regulations

There is a big difference in the overall regulation of surveillance technologies across the nations and the world. Even though certain countries have enacted data protection measures such as GDPR in the EU as well as mechanisms for surveillance oversight, most of these are absent in the laws of majority of other states particularly those in the developing countries. Moreover, the world wide nature of internet and surveillance systems has made it not easy to set uniform regulations to safeguard privacy across borders.[44]

3. Human Rights Implications

Surveillance forms of technologies frequently contravene human rights principles, including the right to privacy, as stipulated with international instruments such as UDHR, ICCPR and regional human rights instruments. The development of state surveillance powers, more so in non-democratic regimes, can threaten civil liberties, freedom of expression and expression of assembly. That the chilling effect that surveillance has on free expression and democratic participation is of major concern.[45]

4. Ethical and Social Concerns

Ethical concerns are also raised by the use of the emerging surveillance technologies viz bias, discrimination and social exclusion. Technologies such as facial recognition and AI-powered predictive policing have a lot of criticism regarding their perpetration of racial, gender and socioeconomic prejudice, culminating in uneven surveillance of the adversely affected communities. The social impact these technologies also have will further entrench inequality and erode public confidence in government institutions.[46]

[44] United Nations, *Report of the Special Rapporteur on the Right to Privacy*, 2018
[45] *Privacy and Human Rights: An International Survey of Privacy Laws and Developments* (Privacy International, 2010)
[46] *Freedom Online Coalition*, Principles on the Application of Human Rights to Communication Surveillance, 2013

POLICY RECOMMENDATIONS

In order to overcome the legal and ethical challenges of surveillance technologies, it is critical that governments international agencies and civil society work together to effect mandatory legal frameworks and policies. Below are key policy recommendations meant at ameliorating negative impacts of surveillance technologies to privacy:

1. Comprehensive Data Protection Laws Adoption

Governments should provide and enforce robust legal provisions on data protection that have specific provisions on how surveillance technologies can be used. These laws should:

a. Make clear rules for collecting, storing and using the personal data gathered from surveillance.
b. Informal consent should not be used for collecting biometric or other sensitive data from individuals.
c. Make data collection confined to defined, legitimate purposes and it should be subject to auditing and oversight on a regular basis.
d. Produce severe penalties against non-compliance and data breach, which would safeguard the privacy rights of people.

2. Promoting transparency and accountability of surveillance practices.

Governments and private entities should be open about the use of surveillance technologies and data collection methods. To this end, they should:

a. Engage in the publication of periodic reports of surveillance activities, indicating what type of technology is used and for which purposes as well as the protections that exist to ensure privacy.
b. Develop public platforms for discussion and debate about surveillance practices and solicit input from civil society organization; privacy activists; and public.
c. Institute robust oversight mechanisms such as independent audits to prevent the abuse of surveillance practices that may infringe privacy rights or other civil liberties.

d. Opposing bias and discrimination in surveillance technologies.[47]

Policymakers need to do pro-active things to curb bias and prejudices in surveillance mechanisms especially those that are informed by artificial intelligence and facial recognition. These steps include:

a. Ensuring that technologies of surveillance undergo stringent testing and validation, so that they do not create disproportionately high burdens on underrepresented groups, for instance racial minorities, women, and economically underprivileged citizens.
b. Oblige surveillance systems to undergo periodic review for possible bias and prescribe corrective action in their remit if required.
c. Promoting the formulation of ethical regulations for the design, implementation and use of surveillance technologies, based on their fairness and non-discrimination.[48]

[47] *Universal Declaration of Human Rights* (UDHR), Art. 12, adopted 10 December 1948, United Nations General Assembly, A/RES/217(III)
[48] Arvind Narayanan and Vitaly Shmatikov, 'Robust De-anonymization of Large Sparse Datasets', (2008) IEEE Symposium on Security and Privacy.