Journal of Carcinogenesis
Covering Genesis to Therapeutics
Journal of Carcinogenesis, ISSN: 1477-3163
2025; Vol 24: Issue 9s, https://carcinogenesis.com/

Surveillance Theories and Its Legal and Social Implications

Mr .M Laxmi Jagannadh[1], Pro S Sumithra[*2]

[1]Research Scholar, Dr BR Ambedar College of Law, Andhar University

[*2]Research Scholar, Dr BR Ambedar College of Law, Andhar University

***Corresponding Author:**

Pro S Sumithra

Email ID: shobana234@gmail.com

ABSTRACT

The study examines how monitoring is changing in India with an emphasis on the system's ethical and legal ramifications. Several theoretical stances, such as utilitarianism, panopticism, social contract theory, and liberal rights theory, are employed to examine the arguments for monitoring. The study also looks at India's domestic legal system, highlighting important rulings like Puttaswamy that acknowledged privacy as a right to life and liberty. It also looks at how India's international commitments under the UDHR and ICCPR are affected by domestic legal instruments. To strike a balance between state interests and constitutional liberties, the document suggests extensive legislation, strong checks and balances, and enhanced data protection.

How to Cite: Mr .M Laxmi Jagannadh, Pro S Sumithra, (2025) Surveillance Theories and Its Legal and Social Implications, *Journal of Carcinogenesis*, *Vol.24, No.9s*, 279-283

1. INTRODUCTION

In an interview with The Guardian, United States government whistleblower Edward Snowden said that he would not want to live in a world where everything one said or did, where everyone one talked to and all forms of creativity or expression would be recorded. This was after he leaked massive Intel on how the US government was running surveillance programs on its citizen's data. He justified his conduct by arguing that the people were entitled to be informed about the power abuse by the government.[1] Hours later at a press conference, the then President Barrack Obama defended the government by putting across that citizens were not to expect perfect security and also expect perfect privacy at no inconvenience. He urged that as a society, choices had to be made. This situation in United States shed light on the issue of surveillance globally.[2]

Surveillance has been a tool for Statesmanship for over centuries and with the emergence and reign of technology in this 21st century, it has profoundly adapted to the modern world. Prior to tech advancements, surveillance was restricted to physical observations, informants, tracking and inceptions that catered for specific target audience.[3] As was observed by Justice Sotomayor, prior to the use of computers, the greatest protections of privacy were practical as opposed to written laws.[4] Due to the wide use of technology and internet, keeping safe of personal information has become a critical issue. Globally, effective regulation makes surveillance vital for national security and the curbing of criminal offences. However, with the battle between security and right to privacy, the boundary between the two has become opaque and raised serious legal and ethical questions.[5]

India is the leading democratic state globally. However, due to technological evolution that has affected the globe, it has also been affected by surveillance issue that has been raised over the programs being operated and the surveillance procedures being followed by the authorities, corporations and individuals with limited transparency and illegally raising legal and ethical queries.

[1] The Guardian, *Edward Snowden: the whistleblower behind the NSA surveillance revelations*, (2013) < https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance> accessed 17 September 2025.
[2] Politico, *Obama defends surveillance* (2013) < https://www.politico.com/story/2013/06/obama-nsa-surveillance-092410> accessed 17 September 2025.
[3] Waldo J, *'A Short History of Surveillance and Privacy in the United States', Engaging Privacy and Information Technology in a Digital Age* (National Academies Press 2007).
[4] *United States v Jones* 565 US 400 (2012).
[5] Aksietha R, *Surveillance in India and its Privacy Challenges in Digital Age: A Legal And Constitutional Analysis* (Christ University 2025).

2. THEORITICAL FRAMEWORK

This paper analyses four relevant theories that have been employed to understand the place of surveillance in our societies by either justifying or critiquing it. Each theory will attempt to provide moral, political and social compasses of the topic. The theories include the social contract theory, utilitarianism, panopticism and liberal rights.

2.1 SOCIAL CONTRACT THEORY

Thomas Hobbes depicted a violent and disorderly society in which people lived solitary, impoverished, cruel, and brief lives. He wrote of a society where men were driven by selfish interest and competed to survive due to the limited resources that nature provided. However, over time, man discovered through reason that he possessed natural rights and thus agreed to form a society based on a social contract theory where a legitimate authority would be established. For there to be peace and security, man had to surrender certain rights to the absolute authority and the authority in exchange would enforce peace and security. Citizens were then required to obey laws and accept their limited rights.[6]

Jean Jacques Rousseau however did not see the world from a negative perspective as Hobbes did. Rousseau wrote of nature as peaceful where resources were abundant. That man was good but society corrupted him. Therefore, through the social contract, man formed a democratic legitimate government based on the general will of all involved. The obedience would not be driven by force but by the general will to live in a peaceful society.[7]

The two theorists may differ in their views of nature however similar content can be derived from their works. That there are laws that form the foundations of liberties for citizens and duties of the Authorities to respect, protect and fulfill these liberties. Surveillance is a security matter. It facilitates the safety of citizens and their states but when it is used as a weapon by the state against its citizens; it becomes a matter of contention.

2.2 UTILITARIANISM AND PANOPTICISM

Jeremy Bentham speaks of pleasure and pain that drive human actions either by encouraging or deterring them. He writes of the greatest benefit for the largest number. He uses the analogy of a panopticon, a central tower in a prison where a guard is stationed to observe prisoners. The prisoners in this situation are not sure when they are being watched and will therefore strive to behave properly. For the security guard, surveillance is what is good for all prisoners because they will be well behaved and this will translate to peace and order. In this situation, surveillance is good for the prisoners.[8] However, Michel Foucault, basing his theory on the panopticon, draws that in the current world, people do not know that they are being watched. This radical view departs from the notion that surveillance is for the welfare and security of citizens and concludes that it is about power and control thus limiting the liberties of citizens.[9]

David Lyon builds on Foucault's theory. However instead of the central and physical surveillance seen in schools, hospitals and prisons as Foucault explains, Lyon writes of how decentralized surveillance has become due to the advancements in Technology. He explains that corporations and even ordinary people have taken up surveillance.[10]

Surveillance has become a vital aspect of maintaining security and order in various aspects of society, both positively as the government portrays it and negatively as criticized by individuals and civil groups.

2.3 LIBERAL RIGHTS THEORY

John Stuart Mill writes of the importance of upholding individual freedoms. He illustrates that the only time power in a civilized society can be used against its member rightfully, is when harm to others occurs.[11]

Ronald Dworkin termed rights as 'trumps' against the state. That individual rights and freedoms will always be important compared to the utilitarian consideration of the majority. He emphasized that surveillance should be subject to legality, checks and balances.[12]

Joel Feinberg writes on the consideration of the seriousness of an offence where rights and freedoms will be interfered with. He considered two factors when surveillance comes to play: seriousness of the offence to be prevented and the extent of the liberty infringed.[13]

Liberal theorists emphasize the significance of individual liberties in society and how interferences with these liberties can

[6] Hobbes T, *Leviathan* (Cambridge University Press 1991).
[7] Rousseau JJ, *The Social Contract* (Cambridge University Press 1997).
[8] Bentham J, *An Introduction to the Principles of Morals and Legislation* (Oxford University Press 1996).
[9] Foucault M, *Discipline and Punish: The Birth of the Prison* (Vintage Books 1977).
[10] Lyon D, *Surveillance Society* (Open University Press 2001).
[11] Mill J S, *On Liberty and Other Essays* (Oxford University Press 1991).
[12] Dworkin R, *Taking Rights Seriously* (Harvard University Press 1977).
[13] Feinberg J, *Harm to Others* (Oxford University Press 1987).

be fatal in protecting citizens from the chilling effects of surveillance.

3. INTERNATIONAL AND DOMESTIC LEGAL FRAMEWORK

3.1 INTERNATIONAL LEGAL FRAMEWORK

Rights have been a crucial part of every society. They have been defined as entitlement to which every person subscribes to de facto of being human. India joined the United Nations in 1945 as a founding member. In 1948, The United Nations General Assembly embraced the Universal Declaration on Human Rights and in 1979; India approved the International Convention on Civil and Political Rights thus giving rise to its obligation to the international sphere. International obligations do not mandate member states to include their provisions in their domestic laws but rather advocate that member states do include them to achieve some universality especially in matters of respecting, protecting and fulfilling human rights.[14] Indian courts have cited these international instruments in their decisions. Rulings given by the International Court of Justice do not also form binding precedents but are rather persuasive in the formation of state judgments.

3.2 THE UNIVERSAL DECLARATION ON HUMAN RIGHTS (UDHR)

This is the bedrock instrument in matters of setting the framework for human rights globally, multiple regional and domestic state laws. It was generally adopted by member states of the UN but it cannot be ratified.[15] However, since other UN human rights instruments stem from it, member states are required to ratify the subsequent instruments.

The following provisions relate to rights and fundamental freedoms that have been threatened, denied or violated when surveillance has been used to instigate a culture of fear and distrust rather than security. Article 12 shields information, family, home, and privacy from intrusion. Freedom of opinion, conscience, and religion, as well as the right to change in private or in public, are all protected under Article 13. Article 19 allows for opinion and expression, peaceful assembly, and participation in governments through chosen leaders.

3.2.1 INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS

As a subsequent instrument fashioned to give essence to not only the UDHR in theory but also in practice, the United Nations Human Rights Committee[16] was established to handle cases involving states versus states, individuals versus states, civil organizations versus states and so on. In summary, Articles 17 articulates the privacy right and Article 18 emphasizes the freedom of religion, thought, and conscience. Article 19 addresses freedom of expression and opinion while Article 22 and 25 outline the privacy rights, associational liberties and public participation respectively. These provisions are similar in writing to those of the UDHR.

The general comment by The Human Rights Committee emphasized that though privacy interference is allowed it must be lawful, non-arbitrary, and reasonable, with limited exceptions. The general comment suggests that there should be laws that specify exactly what these circumstances are. Competent bodies with the authority of Law are to make such decisions that permit interference to this right. Integrity and confidentiality are principles that been emphasized for compliance to privacy. The comment goes ahead to strongly prohibit surveillance through interception of telecommunication. Searches for homes are allowed only where there is a warrant and is restricted to the collection of evidence and harassment has been condemned. For body searches, respecting human dignity should be upheld. Access to personal data should be legal, secure, and subject to consent. States should have accessible remedies in case of privacy interference. [17]

Following the whistleblower Edward Snowden leaked information about the use of programs such as PRISM for surveillance by USA government, the Human Rights Committee in its concluding observation raised concerns over the limited protection of rights versus the excessive surveillance on the grounds of national security. Also raised as concerns, the lack of oversight by the judiciary, disproportionate collection of data and discrimination of non-citizens were noted.

3.3 INDIA'S LEGAL FRAMEWORK

3.3.1 CONSTITUTION

India's constitution doesn't expressly provide for the right to privacy. Indian courts had previously rejected any notion that privacy was a constitutional right; this is evidenced by cases such as *M.P. Sharma v Satish Chandra*[18] where privacy was

[14] Henry S, *Basic Rights: Subsistence, Affluence, and U.S. Foreign Policy* (Princeton University Press 1980).
[15] UNGA Res 217 A (III) *Universal Declaration of Human Rights* (10 December 1948) UN Doc A/RES/217(III); Philip Alston and Ryan Goodman, *International Human Rights* (4th edn, Oxford University Press 2021) 150; United Nations, *Universal Declaration of Human Rights* (United Nations Human Rights Office of the High Commissioner, 2023) https://www.ohchr.org/en/universal-declaration-of-human-rights accessed 17 September 2025.

[16] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR) Article 28.
[17] Human Rights Committee, *General Comment No 16: Article 17 (Right to Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation)* (8 April 1988) UN Doc HRI/GEN/1/Rev.9 (Vol I).
[18] *M.P. Sharma v Satish Chandra AIR* 1954 SC 300, 1954 SCR 1077 (India) 1087.

raised after a company's information was collected after searches and seizures. The court observed that if the legislative body has not included a fundamental right in the law, then the judiciary cannot purport to interpret it. It is nonexistent and by a law being law in a different jurisdiction, it doesn't warrant the same law being a law in another jurisdiction.

However the case of Puttaswamy, a nine judge bench rejected this view and reaffirmed that though not expressly written in the constitution, privacy rights are intrinsic to the right to life and liberty under Article 21. In its judgment, the court also noted the impacts that modern technology has had on state surveillance, digital footprints left online by citizens and profiling and how these have invaded privacy. Though the three advocate for public interests and promote security, especially profiling, they have resulted to discrimination. The court also illustrated ad raised concerns over how the Big Brother State theory through possession and control of data by state. The bench stressed on the need to have a fulcrum between citizen's liberties and surveillance technology.

A proportionality test was adopted and later redefined to build on the parameters for determination of the infringing measures on the constitutionality of privacy to include: legality, purpose, suitability, necessity and procedural safeguards.

Regardless of failure to expressly provide for privacy rights in the constitution, rights such as those of speech, association, and conscience/religion are fundamental and expressly provided for. Surveillance without oversight tends to breach the constitutionality of these rights.[19]

3.3.2 LEGISLATIVE FRAMEWORK

The primary statutes that govern surveillance in India include the Telegraph Act 1885, the Information technology Act 2000 and their subsequent rules. The presence of Telecom and internet service providers in India necessitate the need for licensees from Government to allow them operate. These licenses contractually bind the service providers to include obligating them to cooperate with law enforcers when surveillance matters arise. Criminal and civil law through the Criminal Procedure Code and the India Evidence Act have also built the architecture on surveillance in matters of investigations and admissibility of intercepted communications in courts.

The Telegraph Act describes telegraph[20] as any form of communication, wired or wireless. This broad definition includes any and all other forms of communication in existence.

The Act authorizes government to temporarily possess proceeds of communications in circumstances: where public safety is necessary, protection of a country's sovereignty and integrity, its diplomatic ties with other states, for order and prevention of instigation to commit offences.[21]

The Indian Telegraph Rules 1951 specifically Rule 491A provide the procedures that ought to be followed where Section 5 of the Act is invoked. Briefly, the procedures entails that the Secretary to the Government is required by the Act, to issue interception directives. These are valid for a maximum of sixty days and require approval from the head most office of the authorized security. Internal controls must established by service providers to guard against illegal surveillance and preserve confidentiality. Records are destroyed every six months, and the Review Committee evaluates these guidelines once a month.

The Information Technology Act 2000 was aimed at promoting India's economic growth by overseeing the digital sphere to include its ecosystem, e-communications, cybercrimes, and security practices. It gave the government the authority to conduct surveillance directly through appointing its own officials and indirectly through intermediaries and cyber cafes, thus ensuring citizen safety.[22] The Act also establishes the India Computer Emergency Response Team[23] that can demand for information and give directions for cyber security purposes. Following the recent directions in 2022,[24] the CERT-IN directions require that Virtual Private Networks and Virtual Private Server providers keep records for subscribers and their activities. Moreover, Information Communication Systems are obligated to keep log information for One hundred and eighty days.

This Act outlines that for India's sovereignty, integrity, defense, security, and public order, the Central or State Government may give instructions for the interception, monitoring, or decryption of information using computer resources. For safe access, the middleman must offer technical support. Public access to data created, sent, received, saved, or hosted on computer resources may also be restricted by the central government. Intermediaries may offer technical support while agencies watch and gather traffic data for cyber security. Infractions carry a fine and a maximum sentence of three years in prison.[25]

In 2009, India's parliament passed and amended Act that included provision to allow the intercepting, monitoring,

[19] Indian Constitution 1950, Articles 19 & 25.
[20] Indian Telegraph Act 1885, S. 2.
[21] Indian telegraph Act 1885, S. 5(1).
[22] Information Technology Act 2000, S 17 & S 6A.
[23] Information Technology Act 2000, S 70(B).
[24] CERT-IN, *Methods of Verification to Compliance with Cyber Security Directions of Government of India* (CERT-IN 2022)
[25] Information Technology Act 2000, S 69, 69A & 69B.

decrypting of communication and surveillance of internet traffic data. Personal data safe keeping and the responsibilities of service providers are also envisaged in the Information Technology (Amendment) Act 2008.

The Indian Information Technology Traffic Data Rules 2009, details the procedures that competent authorities and intermediaries should follow as well as the principles that should be adhered to. The Indian Information Technology (Intermediary Guidelines and Digital Media Ethics Code) 2021mandates that service providers have to cooperate with authorities through making available any and all necessary information, materials and resources within a prescribed time, to give room for the verification of users, curbing, investigating, and prosecuting law-related offenses.[26]

Information Technology (Guidelines for Cyber Cafe) Rules, 2011 authorizes owners of cyber cafes to cooperate with authorized officers and provide information on demand during inspections.[27]

Courts and law enforcement can request papers for trial, including information from postal and telegraph agencies, under the 1973 Code of Criminal Procedures (CrPC).[28] Moreover, the 1999 Maharashtra Control of Terrorism and Organized Crimes Act establishes its own protocols and gives its agents the power to conduct surveillance. On the admissibility of evidence collected through and from surveillance, the 1967 Unlawful Activities Prevention Act (UAPA) legalizes such evidence. As per the Criminal Procedure (Identification) Act 2022, persons in conflict with the law at law enforcement facilities to include detention and police stations may have their fingerprints and photos taken, and these records may be retained for a maximum of 75 years.

4. TYPES OF MODERN SURVEILLANCE USED INDIA

The Central Monitoring System that allows for bulk collection of data and analysis of communications. The Network Traffic Analysis is designed to pick up pre-defined key words in real time internet traffic such ‘bomb’. The National Intelligence Grid has been used to sum up data from twenty one classes from tax, banking and transport to allow for economic monitoring and enforcement of the law. The Crime and Criminal Tracking Network System has enabled for interlinking of police stations forming a database of crimes and criminals’ network. This has facilitated the Automated Facial Recognition Systems that uses images for surveillance.[29]

The Aadhaar Act 2016[30] has been criticized by the Supreme Court and noted to be a double edged sword. Though supporting government initiatives for citizens, the Act posed serious challenges to the Liberty of citizens. The Supreme Court advised the legislature to strike down provisions that interfere with the constitutional rights of citizens especially privacy and impose constraints on the Aadhaar operations.

5. CONCLUSION

It is evident that surveillance though positive has its own flaws. A perfect balance between national security/interests and individual liberties may never be achieved but purposed attempts can be made. Therefore, this paper makes the following recommendations.

First is to establish a system of checks and balances. An impartial judicial system should be empowered to counter the executive dominated reviewing processes. Media, which a big part in ensuring that democracy is upheld by reporting on government’s actions should also be empowered and not interfered with. Second, comprehensive legislations should be adopted either by repealing or amending the two ancient statutes. This will allow for current legislations that align with current judicial guidelines such as the proportionality parameters set out in the Puttaswamy case. Third, will be the strengthening of data protection both through legislation, policies and precedents. Principles of data protection specifically personal data need to be adhered to. International instruments advocate for these and so should domestic laws.

---

[26] Intermediary Guidelines 2021, Rule 3(1) (j).
[27] Guidelines for Cyber café 2011, Rule 7.
[28] Code of Criminal Procedures 1973, Section 91 & 92.
[29] Center for Communication Governance, *The Surveillance Law Landscape in India and the Impact of Puttaswamy* (National Law University Delhi Press 2023) < https://ssrn.com/abstract=4624419> accessed 16 September 2025.
[30] Wanjiku F, ‘*The Aadhaar Act affords unique identity to individuals to ensure that such government subsidies, benefits and services reach only the intended beneficiaries and thus upholds the concept of limited government, good governance and constitutional trust* (Kenya Law, 16 August 2019).