Jus Corpus Law Journal
Open Access Law Journal – Copyright © 2024 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey



# Wiretapping in India: Understanding its Laws and Implications

Dhriti Kawale[a]

[a]University of Mumbai Law Academy, Mumbai, India

*Received* 03 February 2024; *Accepted* 26 February 2024; *Published* 29 February 2024

*Technology has made wiretapping a major national security and privacy issue. Monitoring phone calls, texts, and emails may violate private rights, requiring legislation and legal control. This paper examines wiretapping's legality and the need for rules to limit use. It also examines how the judiciary sets wiretapped evidence standards. A comprehensive analysis of US and Indian wiretapping laws and regulations is the research design. Unauthorised communication eavesdropping is examined through wiretapping case studies and court verdicts. Wiretapping is legal and ethical implications for national security and privacy are considered. The analysis indicates that wiretapping regulations are necessary for national security but may breach private rights. Law enforcement and oversight are essential to preventing power abuse. The paper also suggests balancing law enforcement efficiency and privacy. The findings emphasise the need to balance national security and privacy in wiretapping regulation. Legal safeguards and oversight are needed to prevent wiretapping for spying, according to the report.*

**Keywords:** *wiretapping regulations, security and privacy, legislation control, judiciary.*

## INTRODUCTION

In recent years, there has been a significant amount of advancement in the field of technology. Technology unquestionably possesses several advantages, but just like every other phenomenon, it also possesses several disadvantages. The advancement of technology has

resulted in a significant reduction in the size of the world. We are still able to communicate with someone at one thousand miles by sending them an email, calling them, or sending them a text message. In conjunction with this, the issue of safety comes into play. Recent years have seen an increase in the frequency with which the government's practice of monitoring the phone calls, texts, and emails of its citizens for the sake of ensuring national security. The most obvious problem is whether this violates the right of individuals to have their privacy protected.

Phone tapping, which is defined as 'the activity of secretly fitting a special device to someone's phone in order to listen to their phone conversations without being noticed,' is one consequence of technological progress that many people have failed to take into consideration. In relation to the topic at hand, the formation of rules and regulations, in addition to a legal framework, is of the utmost significance. For the purpose of determining the extent to which it will be legal to listen in on phone calls or to listen in on any other sort of communication, the government ought to enact regulations that specify the extent to which this will be permitted. In addition, it is of the utmost necessity that the Judiciary create norms regarding the utilization of this material as a sources of evidence. All of these norms should be established.

**WHAT IS WIRETAPPING/PHONE TAPPING?**

Wiretapping is the procedure by which one person or party secretly listens to the conversation of another party across a wired or wireless network. Communication equipment may include a **telephone line, a fax machine, a computer, or other gadgets.** In the decades leading up to the 1960s, law enforcement officials were not obliged to get a warrant to listen in on any conversation. Later, the Supreme Court of the United States of America concluded that individuals have a reasonable expectation of privacy in their phone conversations and that law enforcement must first acquire a search warrant before they can wiretap telephone conversations.

In recent years, police enforcement has utilized a wide variety of state wiretapping statutes in a variety of unconventional methods to apprehend persons who are secretly recording other individuals with video cameras that also record audio. For the purposes of this discussion,

'secretly' may simply refer to recording the individual without obtaining their permission. It is possible that the rules governing wiretapping differ from state to state; therefore, it may be beneficial to check with a local attorney to ascertain which laws are applicable in a particular place.

It is claimed that telephonic equipment, along with other communication devices, are included in the Union List of the Constitution, entry 31, and the Federal List of the Government of India Act, 1935, entry 7.[1] In accordance with the provisions of Section 5(2) of the Indian Telegraphic Act 1885[2], the State Government as well as the Central Government have the authority to bug the telephones of individuals. During an investigation, there are instances in which it is necessary for the authority or agency to record the conversation of a person who is being investigated. Before being able to listen in on the person's phone calls, these authorities are required to obtain permission from the Ministry of the Home. Whenever an agency or authority applies to the Ministry, they are required to provide a justification and a list of the need for tapping phone calls. It is necessary to obtain approval from the State Home Secretary if the state is involved. Communication between political leaders that takes place over the phone cannot be legally intercepted.

**HISTORY OF WIRETAPPING**

The balancing of individual rights with state and law enforcement concerns regarding wiretapping rules has consistently posed challenges. Wiretapping, which involves the interception of telegraphic communications, has been employed since the inception of the telegraph. However, the initial utilization of wiretapping by law enforcement authorities occurred in the 1890s in New York City[3]. The New York State Department uncovered that during the 1910s, officers had engaged in the unauthorized practice of wiretapping entire hotels, without obtaining a warrant.

[1] HM Seervai, *Constitutional Law of India* (4th edn, Universal Law Publishing 1996)
[2] Indian Telegraphic Act 1885, s 5(2)
[3] Howard J. Kaplan et al., 'The History and Law of Wiretapping' (ABA Section of Litigation 2012 Section Annual Conference, April 18-20, 2012)

The department contended that it did not breach any Fourth Amendment rights[4], as the Fourth Amendment primarily safeguards verbal communications, such as mail, and considers the act of placing taps as trespassing. The Foreign Intelligence Surveillance Act (FISA) was enacted in 1978 with the aim of granting wiretap orders in cases related to national security.[5]

## INTER-RELATION BETWEEN PHONE TAPPING AND THE RIGHT TO PRIVACY

Although there are numerous opinions about wiretapping, which, depending on your intentions, can be used for good or evil, let us refrain from discussing its moral or ethical implications for the time being and focus on its legal aspects.

**Wiretapping and phone tapping are closely associated with the 'Right to Privacy' as outlined in Article 21:** Telephone tapping or wiretapping refers to the clandestine attempt to surveil an individual's phone conversations by means of an accessory that is surreptitiously affixed to the device. In India, the ability to surveil phones or other electronic devices is restricted to a select group of specialized authorities, including the government. Such tapping is permitted only under extremely specific conditions that safeguard the security of the nation or state and preserve public order and safety in the face of dangers such as lynchings, among others. Private individuals or organizations are prohibited by government regulations from surveilling private conversations or tapping phones; doing so would infringe upon individual privacy.

However, there were only a few instances of the right to privacy being codified at the time that the Indian constitution was being drafted. For example, the privacy theory was never explicitly mentioned in common law until much later. When it comes to the right to privacy, **Jude Cooley** emphasizes that it is equivalent to the right to be left alone[6]. In **Kharak Singh v State of Uttar**

[4] '4th Amendment' (*Historical Society of the New York Courts*) <https://history.nycourts.gov/democracy-teacher-toolkit/criminal-law-civil-liberties/4th-amendment/> accessed 01 February 2024

[5] James G. McAdams III, Foreign Intelligence Surveillance Act (FISA): An Overview (*Bureau Of Justice Assistance*) <https://www.fletc.gov/sites/default/files/imported_files/training/programs/legal-division/downloads-articles-and-faqs/research-by-subject/miscellaneous/ForeignIntelligenceSurveillanceAct.pdf#:~:text=In%201978%2C%20it%20presented%20the%20Foreign%20Intelligence%20Surveillance,purpose%20of%20collecting%20foreign%20intelligence%20and%2For%20foreign%20counterintelligence> accessed 01 February 2024

[6] Thomas M Cooley, *A Treatise on the law of torts* (2nd edn, Callaghan and Company 1888)

**Pradesh,**[7] the court studied the relationship between surveillance and personal and concluded that an unauthorized intrusion into a person's house would interfere with his or her right to personal liberty. This was the beginning of the process that is tied to the right to privacy.

Unauthorized entry into residences was considered an infringement on the right to personal liberty, as the right to privacy was originally envisaged in relation to the home. It was proclaimed that the right of the people to be secure in their persons, dwellings, papers, and effects could not be violated, and the court acknowledged this. In a unanimous decision, the court found that absent a legally authorized procedure, tapping someone's phone would be a violation of both Article 21[8] and Article 19[9] that guarantees citizens' rights to free speech and assembly respectively.

In addition, the Supreme Court made it clear that laws defining when interception can occur still need procedural support to guarantee that the use of authority is fair and reasonable.[10] When it comes to the taking away of someone's life or freedom, Article 21 considers the legal process. The courts will ensure that no one can illegally or overly pryingly listen in on a private citizen's phone call. No one is shielded from the police's attempts to uphold the law and root out corruption among public officials, even if they are guilty. It is important to note that the courts will not stand by and let the police use illegal or irregular procedures even if it means endangering safeguards meant to protect citizens.

In this instance, there is no way that is illegal or even irregular that may be used to obtain the cassette recording of the conversation. The right to privacy may be subject to limitations in certain circumstances, such as when there is a compelling state interest that needs to be fulfilled and when there is a significant countervailing interest that is superior to the right to privacy.

[7] *Kharak Singh v The State of U. P. & Ors* AIR 1963 SC 1295
[8] Constitution of India 1950, art 21
[9] Constitution of India 1950, art 19
[10] *People's Union Of Civil Liberties v Union of India* (1997) 1 SCC 301

## IS A WARRANT NEEDED FOR WIRETAPPING?

Contrary to the portrayal in movies and television, wiretapping by police enforcement is infrequent. Law enforcement agencies can employ wiretaps under specific situations, and these surveillance techniques serve as valuable tools for their operations. When people think about wiretapping, they typically envision the interception of a phone call or the recording of a face-to-face conversation. Wiretapping laws encompass all forms of oral, wire, and electronic communications that are intercepted by police enforcement.

Law enforcement is subject to federal regulations regarding wiretapping. The Federal Wiretap Act prohibits the interception or disclosure of wire, oral, and electronic communications. This legislation also forbids the production, ownership, and dissemination of interception devices. The legislation grants federal and state government agencies the power to legally intercept, utilise, and reveal data of communications in specific criminal investigations.

Among the various forms of communication that are susceptible to being intercepted, divulged, and utilized are **e-mails, faxes, pager numbers, and telephone calls**. Under specific circumstances that are subject to stringent regulations, prosecutors can incorporate communications that were collected through wiretapping as evidence in court. Wiretaps are a tool that law enforcement agencies can employ to investigate a variety of crimes, including **kidnapping, homicide, and white-collar crimes.**

On the other hand, it is most frequently utilized in the process of investigating and prosecuting instances that involve restricted substances. Within the context of criminal investigations, the act specifies the kinds of investigations that can make use of wiretaps. According to the statute, state officials have the authority to request an investigation into a wide range of crimes, such as murder, kidnapping, drug dealing, and other offences that pose a threat to life, limb, or property and carry a sentence of more than one year in prison.

During their investigations into felonies, federal law enforcement is authorized to make use of wiretaps. However, when it comes to wire or oral intercepts, they are restricted to investigations that are specifically stated in a statute that is a part of the Act. The requirements for wiretapping

warrants stipulate that for law enforcement agents to obtain a warrant for wiretapping, they are required to follow a set of procedural steps. It is possible that a criminal case would be dismissed if these processes are not followed. This is because the prosecution would not be able to use the wiretap evidence that was gathered during the trial.

## ACTS THAT TALK ABOUT WIRETAPPING/PHONE TAPPING

**1. Indian Telegraph Act 1885:** It was during the time of British colonial authority that the Indian Telegraph Act was enacted. Since then, it has undergone numerous amendments in order to accommodate the development of modern communication technology. Following the provisions of this legislation, the government is granted the ability to intercept and monitor telegraph communications, which includes discussions over the telephone and communications over the Internet. The act permits legitimate interception for a variety of reasons, including the public's safety, the nation's security, and the prevention of criminal activity.

On the other hand, it establishes protocols and prerequisites to guarantee that the act of interception is carried out solely for authorized reasons.

**2. Information Technology Act 2000:** India's Information Technology Act is largely concerned with the regulation of electronic communication and the protection of data. Provisions pertaining to the interception, monitoring, and decryption of electronic information are included in this document. If it is deemed necessary in the interests of the sovereignty and integrity of India, defense of India, security of the state, friendly relations with foreign states, or to prevent incitement to the commission of any cognizable offence, the government is granted the authority to intercept, monitor, and decrypt information that is generated, transmitted, received, or stored in any computer resource. This authority is granted by Section 69 of the Information Technology Act. As was the case with the Indian Telegraph Act, the Information Technology Act places an emphasis on the necessity of obtaining the appropriate authorization and adhering to the processes that have been defined for conducting interceptions.

While the practice of mass monitoring is often regarded as illegal, the practice of individual surveillance is not only legal but also subject to certain restrictions. Nevertheless, the most

challenging aspect is when surveillance is concerned with matters of national security significance. This occurs more frequently in regions that are bordered by Naxalist territories or in places that are prone to Nasalism, where surveillance is significantly stricter and telephone tapping is more pervasive. Even intelligence services like the RAW are granted the authority to prescribe phone tapping, and even though this may constitute an invasion of an individual's right to privacy, it is justified on the grounds of the broader public good or for the sake of public safety. Phone tapping is a notorious practice, and even though privacy is acknowledged as an essential component of the right to life, the Indian approach to surveillance or prescribing phone tapping has not been seen to have circumscribed. This is because the Information Technology Act permits wiretapping to go beyond national security interests in order to even investigate or prevent offences from being committed.

**PROS OF WIRETAPPING LAWS**

**1. Law Enforcement Tool:** When conducting criminal investigations, wiretapping can be an invaluable tool for law enforcement. The apprehending of offenders and an increase in public safety can result from its use in both the prevention and solving of crimes.

**2. Protection of Privacy:** If they are properly enforced, rules pertaining to wiretapping have the potential to protect the right of persons to privacy by imposing limitations on the unauthorized surveillance and interception of communications.

**3. National Security:** In situations where there is a threat to national security, it may be essential for intelligence services to engage in wiretapping in order to monitor and prevent prospective acts of espionage or instances of terrorist activity.

**4. Legal Oversight:** In several nations, the act of wiretapping is subject to stringent legal control, which indicates that law enforcement agencies are required to seek warrants from the courts before conducting surveillance. The prevention of abuses and the guarantee that wiretapping is carried out for lawful reasons are both provided by this.

## CONS OF WIRETAPPING LAWS

**1. Concerns Regarding Privacy:** It is possible for wiretapping to violate the right of persons to privacy, which can result in a sense of being watched and the development of mistrust. When wiretapping is carried out without proper oversight or authorization, it can violate civil freedoms and lead to abuses of power.

**2. Potential for Abuse of Power:** There is a possibility that law enforcement or government agencies could abuse the power of wiretapping in order to engage in unauthorised monitoring, pursue political advantage, or harass individuals.

**3. Illusion of Safety and Confidence:** It is possible that wiretapping is a technique that can be used to combat criminal activity; nevertheless, the success of this instrument is not always guaranteed, and criminals may find ways to communicate in a secure manner or to avoid being monitored.

**4. The Problems Caused by Technology:** The proper regulation of wiretapping is becoming increasingly difficult to achieve as technology continues to advance. The use of sophisticated encryption and communication methods can make it more difficult to conduct surveillance, which may result in legal gaps.

**5. Concerns Regarding the Universe:** The laws and regulations governing wiretapping vary from country to country, which makes it difficult to conduct conversations across international borders. It is possible that this will give rise to concerns regarding international cooperation and jurisdiction. Legislation pertaining to wiretapping can be a sensitive issue since it requires striking a balance between the necessity for efficient law enforcement and national security and the preservation of individual privacy and civil freedoms. Legislators and society as a whole face a constant challenge in the form of the desire to find a solution that strikes a balance between these competing interests.

## SAFEGUARDS AGAINST PHONE TAPPING

**1. Substantive Safeguards:** Although the Court did not find Section 5 (2) to be unconstitutional, they did acknowledge the fact that there were no procedural safeguards in place for the substantive requirements. According to the majority opinion of the court, it is of the utmost importance to support the substantive law with some procedural laws. According to the opinion of the Court, the substantive provisions will be rendered invalid if the appropriate procedure is not properly followed. There are also some substantial safeguards that are provided by the Telegraph Act. In accordance with the provisions of Section 25 of the Act, any individual who seeks to intercept or become familiar with any message and tampers with any deception with the intention of doing so shall be punished with a prison sentence that may extend up to three years, a fine, or both.[11]

**2. Procedural Safeguards:** During the course of the previous ten years, numerous scandals concerning the problem of phone tapping have been brought to light. When the situation reached such a high level of intensity, it was transformed into a political agenda. The politicians of opposing parties levelled accusations against one another. On the instruction of the party in power, it was alleged that the government listened in on people's telephone conversations. The People's Union of Civil Liberties (PUCL) submitted a Public Interest Litigation (PIL) to the Supreme Court at that time, demanding that the court provide clarification on the law regarding the issue of electronic tapping and interception[12]. The petitioners argued that the arbitrary power that was granted by Section 5(2)[13] ought to be subject to regulation. In addition, they argued that the alteration that was made to Section 5(2) in 1971 was particularly risky since it permitted interception not only in the event of an emergency and for the purpose of maintaining public order and safety but also for the purpose of inciting offences.

The Supreme Court has acknowledged that the right to privacy is guaranteed by Article 21 of the Constitution and has expressed the opinion that wiretapping constitutes a severe violation

[11] Indian Telegraph Act 1885, s 25
[12] Priyan Garg, 'Law On Phone-tapping In India' (*Academike,* 04 February 2015) <https://www.lawctopus.com/academike/law-phone-tapping-india/> accessed 01 February 2024
[13] Indian Telegraph Act 1885, s 5(2)

of privacy. However, the Court ruled that Section 5 (2) was constitutional.[14] India has likewise pledged its allegiance to the ICCPR, which guarantees its citizens the right to privacy in Article 17.[15] One is also exercising his right to freedom of expression and speech under Article 19 (1) (a) when conversing with another party over the phone. A violation of this clause would result from tapping the call unless there are acceptable restrictions outlined in Article 19 (2). Note that the Supreme Court did not wish to completely do away with the phone tapping system since it believed that in certain instances it is very essential to take a few steps like this for the nation's security. However, the Court did order the formation of an elite committee to investigate the legality of phone tapping.

To control phone tapping following the PUCL case, the Union Government included Rule 491-A in the Indian Telegraphic Rules, 1951. However, the situation was not significantly altered by this revision either.

**PUNISHMENT FOR WIRETAPPING**

If an individual, organization, or government agency engages in illegal wiretapping to intrude upon someone's privacy by eavesdropping on their telephone conversations, the affected individual has the right to submit a formal request to the court. As to Article 26(b) of the Indian Telegraphic Act, anyone who is apprehended for unlawful interception is liable to a three-year imprisonment. Moreover, it would be a breach of the right to privacy as stipulated in Article 21.

**RELEVANT CASE STUDIES**

**1. Mr. Mukesh Kumar Kaushik v/s Delhi State Industrial:**[16] In this instance, the public authorities regularly disclosed the assets of public servants using specialized gadgets. The case

[14] Shaunak Choudhury, 'Fundamental Right to Privacy and Tapping of Telephones' (*Lexforti*, 21 May 2020) <https://lexforti.com/legal-news/fundamental-right-to-privacy-and-tapping-of-telephones/#:~:text=Thus%20section%205%20%282%29%20of%20the%20Indian%20Telegraph,safeguards%20that%20were%20provided%20by%20the%20Supreme%20Court> accessed 01 February 2024

[15] Constitution of India 1950, art 17

[16] *Mukesh Kumar Kaushik v VK Garg* App No CIC/SG/A/2009/001730

gained attention when the plaintiff filed a lawsuit. The Delhi High Court rendered its decision on the wiretapping case.

**2. R M Malkani v/s State of Maharashtra:**[17] The subject of whether a criminal prosecution could be commenced based on a telephonic conversation was discussed in the judicial pronouncement. The purpose of the discussion was to determine whether the conversation could be considered self-incriminating evidence. The subsequent scenario involved a situation in which the Coroner of Mumbai desired to accept a bribe from a physician. Therefore, rather than accepting the money, the physician contacted the Anti-Corruption Bureau. The officials created a trap, and they invited the doctor to have a telephone discussion with the coroner. During that conversation, the coroner made various statements that may be used to incriminate himself, such as the amount of the bribe, the location of the delivery, and other similar things. An audio recording of the conversation was made, and charges were brought against the individual based on the exchange.

The Court, while appreciative of the approach that was taken, came to the realisation that it could potentially pave the way for a great deal of similar activity. The Court went on to say that such methods ought to be utilised in a very limited capacity and only within the appropriate authorization and instruction.

**3. Dharambir v/s Central Bureau of Investigation:**[18] In this particular instance, the Central Bureau of Investigation (CBI) has provided a comprehensive account of the procedure that was followed in order to compile the list of calls that were pertinent to each of the cases. During the process, however, a significant amount of material was gathered by recording the talks that took place over the phone on the hard disc. This information was then converted onto CDs and provided to the accused. Since hard discs were mentioned, it was deemed to fall within the scope of Section 3 of the Electronics Act, when read in conjunction with Section 173(5)(a) and Section 207(v) of the Criminal Procedure Code.

[17] *R. M. Malkani v State of Maharashtra* (1972) 2 SC WR 776
[18] *Dharambir v Central Bureau of Investigation* 148 2008 DLT 289

**4. Sunil Gupta v/s State of Madhya Pradesh:**[19] Within the context of this particular case, the Supreme Court issued a decision about the admissibility of intercepted telephonic calls as evidence in a criminal trial. Additionally, the court addressed the significance of adhering to appropriate protocols when intercepting communications.

## CONCLUDING REMARKS

Technological progress has unquestionably shrunk the globe into a more manageable size. While criminals and terrorists continue to exploit technology for their own ends, the government will inevitably respond by implementing countermeasures, which could inadvertently or purposely pry into our personal lives. One could argue that tapping or intercepting calls, messages, and emails is an unfortunate but necessary evil. Everything is wrong with these kinds of problems because everyone says they shouldn't be, yet no one stops doing it.

In this day of rapid technological development, the danger to personal privacy is real and has grown. Data breaches occur when entities other than state-authorized ones gain access to personal information. The correct precautions must be taken and a balance must be struck between citizen rights and state interests in order to handle such a delicate matter. Concerns over the violation of individuals' rights should take a back seat to more fundamental concerns, such as national security and the prevention of mass casualties. For an agency to justify the use of wiretapping or interception to get data or information, there must be a compelling cause to do so. There is a lack of coordination in wiretapping. When multiple agencies are tasked with monitoring the same number at the same time, it leads to an increase in burden rather than increased efficiency and speed. This problem occurs because there isn't a centralised database that can tell us how many phones are being tapped and by which agency at any one moment. Security services now rely on phone tapping, so it's important that all precautions and regulations be followed to keep everyone secure and prevent any infringement of their rights.

[19] *Sunil Gupta And Ors v State of Madhya Pradesh And Ors* (1990) SCR 2 871

**'Civil liberties are far too important to be left to the executive or the Home Secretary,'** Justice Rajinder Sachar, a former Chief Justice of Delhi High Court, so appropriately puts it.[20] Unintentional tapping could occur if the wrong permissions were granted. Some also contend that the system ought to be modelled like the one in the United States, where a judge, after reviewing the case's merits, authorises sanctions for phone tapping. In most respects, the Supreme Court's ruling is reasonable, and it has established some ground rules. It is possible to overcome the arbitrary nature of any legislation by implementing it correctly, so long as the law serves its intended goal.

Nevertheless, the burden of justifying a law that violates rights grows considering the negative impact that non-implementation has on Indian laws. While wiretapping is still a useful tool for identifying perpetrators of crimes, it must be used appropriately to avoid infringing on anyone's rights and privileges.

[20] Punnet Dhanoa, 'An Analysis of Telephone Tapping as an Investigation' (*SCC Online*, 08 April 2022) <https://www.scconline.com/blog/post/2022/04/08/telephone-tapping-as-an-investigation/> accessed 01 February 2024