DRAFT

Law Enforcement, National Security, and Privacy

Contents

Introduction

This chapter considers the tension that is created between the need of the government to protect the national security of a country, and the protection of individual privacy. The chapter will look at how information collected by law enforcement is processed, handled, stored, accessed and shared, and reviews the privacy implications of legislation that has been put in place to protect the national security of India. As part of this evaluation, the chapter will consider in what circumstances national security should trump individual privacy, under what circumstances does an individual have the right to know when they are under investigation vs. what information can be declared privileged, and what safeguards should be put in place and practiced by relevant actors and stakeholders. The chapter also begins to look at surveillance practices carried out by the government of India, and how these practices impact privacy rights.

Legislation

Unlawful Activities (Prevention) Act, 1967

The Indian government has now withdrawn its two major anti-terror laws which were widely criticized for being draconian and were extremely controversial. However, they realized that the current criminal law regime in the country may not be strong enough to deal with the specific threat of modern day terrorism and therefore amended the Unlawful Activities (Prevention) Act, 1967 to further strengthen that enactment to include certain provisions to allow the law enforcement agencies to deal with the issue of contemporary terrorism.

Oversight

- *Designated Authority*: The Act provides for an officer not below the rank of Joint Secretary (in case of Central Government) or Secretary (in case of State Government) to be notified as a "Designated Authority" which has the power to approve or disapprove orders of attachment of property under the Act.[1] The Designated Authority has all the powers of a civil court required for making and full and fair enquiry of the matters before it.[2]

Collection Limitation

- *Attachment of Property*: Any officer investigating certain offences under the Act has the power, with the prior approval of the Director General of Police, to attach any property which the officer has reason to believe represents the proceeds of terrorism. The Designated Officer within whose jurisdiction the property is situated shall be informed within 48 hours of such seizure of the property, and the Designated Officer is required to either confirm or revoke the order of attachment within 60 days of the production of the property before it, after giving the person whose property is being seized, an opportunity to present his/her case.[3] Similarly the Act gives the Court hearing a case under this Act, the power to attach all moveable and immoveable properties of an accused.[4]
- *Furnishing Information*: An investigating officer investigating an offence, with prior approval from the Superintendent of Police, has the power to order any person (including banks, organizations and companies) to furnish information in relation to the offence and failure to comply with such an order (or furnishing false information) will be punishable with fine or imprisonment upto 3 years or both.[5]
- *Interception*: The Act allows for information collected through interception of communications to be produced as evidence for an offence under this Act.[6] However, the intercepted communication is not admissible unless the accused is given a copy of the order approving the interception, thus making illegal interceptions inadmissible. Therefore unless the interception order itself was obtained by fraud, this provision provided an excellent safeguard against the use of illegally obtained interceptions for evidentiary purposes, sort of neutralizing the ratio of *R.M. Malkani's case*. The

[1] *Id.* section 25.
[2] *Id.* section 31.
[3] *Id.* section 25.
[4] *Id.* section 33.
[5] *Id.* section 43F.
[6] *Id.* section 46.

Prevention of Terrorism Act, 2002 also had admissibility and notice safeguards as well as the probable cause standard incorporated into its interception provisions. These safeguards are not present either in the Telegraph Act, 1885 or the Information Technology Act, 2000.

Notice

- Providing Interception Order: The Act provides that not intercepted communication shall be received in evidence unless the accused is provided a copy of the interception order.

Penalty/Offenses/ Liability/ Remedy

- *Appeal to Tribunal*: Any order made by the Central Government declaring an association as unlawful shall be forwarded to the Tribunal constituted under this Act for determining whether or not there is sufficient cause to declare the association as illegal or not and the Tribunal shall serve a notice upon the concerned association to show cause as to why it should not be declared illegal.[7]
- *Review Committee*: The Act also provides for a Review Committee to which an application may be made by the organization which has been notified as "Unlawful" under the Act or any person who is affected by such a notification for the removal of such organization from the list of unlawful organizations.[8]

Missing Principles

- Openness
- Security
- Disclosure
- Access and Correction
- Purpose Limitation
- Choice and Consent
- Quality/ Verification

The Indian Evidence Act, 1872

The Evidence Act was passed in 1872 and governs what evidence is legally accepted in India, what persons are exempt from disclosing evidence, and what evidence individuals can be compelled to provide.

Disclosure

- *Exemptions from disclosure to courts*: Information that is exempt from disclosure in courts includes communications between married couples without consent from the significant other[9] and communications between legal professionals and their clients during the extent of their employment, unless the communication supports any crime or fraud. [10] These exemptions from disclosure apply irrespective of whether the proceedings

[7] *Id.* section 4.
[8] *Id.* section 36.
9 Indian Evidence Act. s. 122
10 Section 126: No barrister, attorney, pleader or vakil shall at any time be permitted, unless with his client's from disclosing, without their client's express consent, the contents of a) any communication made to them b) any document with which they have become acquainted or c) any advice tendered by them to the client if such

are civil or criminal in nature.

- *Exemption of unpublished records*: The use of unpublished records relating to the affairs of the State are not allowed to be used as evidence in the courts.[11] Despite many rulings on the subject, it is still unclear how wide or narrow the ambit of "affairs of state" is. For instance, if the government maintains routine records about individuals in the course of governance, would these count as "official records relating to affairs of state"

- *Exemption of official communications*: Public officers cannot be compelled to disclose communications made to them in official confidence, when the public interest would suffer by the disclosure.[12] In this provision the public officer is empowered to make the decision as to what constitutes public interest.

- *Production of documents*: A witness summoned to produce a document shall, if it is in his possession or power, bring it to the Court, notwithstanding any objection which there may be to its production or to its admissibility. The validity of any such objection shall be decided on by the Court.[13]

- *Information as to commission of offences*: No Magistrate or Police officer shall be compelled to say whence he got any information as to the commission of any offence, and no Revenue officer shall be compelled to say whence he got any information as to the commission of any offence against the public revenue.[14]

- *Indecent and scandalous questions*: The Court may forbid any question or inquiries which it regards as indecent or scandalous, although such questions or inquiries may have some bearing on the questions before the Court unless they relate to fact in issue or to matters necessary to be known in order to determine whether or not the facts in issue existed.[15]

Indian Penal Code, 1860

This legislation is the predominant criminal code in India. It is a general law that defines and establishes offenses and penalties that are applicable to the whole of India, but is not exhaustive in its listing. Relevant sections related to privacy include:

---

information was received by them "in the course and for the purpose of" their employment. Section 127 extends the scope attorney-client privilege to include any interpreters, clerks and servants of the attorney or barrister.

Section 129 enacts a reciprocal protection and provides that clients shall not be compelled to disclose to the Court any "confidential communication which has taken place between him and his legal professional adviser"

11 Section 123 of Evidence Act declares that "No one shall be permitted to give any evidence derived from unpublished official records relating to any affairs of State, except with the permission of the officer at the head of the department concerned, who shall give or withhold such permission as he thinks fit."

12 Section 124

13 Section 162 Indian Evidence Act

14 Indian Evidence Act s. 125

15 Indian Evidence Act s. s.151

Voyeurism

Offense	Fine	Imprisonment
Any man watching, or capturing the image of a woman engaging in a private act in circumstances where she would usually have the expectation of not being observed, or disseminating such image.[16]	To be determined	One to Three years for first conviction Three to Seven years for second conviction

Stalking

Offense	Fine	Imprisonment
Any man who, (i) follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; or (ii) monitors the use by a woman of the internet, email or any other form of electronic communication, commits the offence of stalking	To be determined	Three years for first conviction Five years for second conviction

It may be noticed that both these offences are limited to a case where the man is the perpetrator and the victim is a woman. This means that a man who has been a victim of stalking or voyeurism then he would not be able to take advantage of these sections. Further the voyeurism section uses the phrase "usually have the expectation of not being watched", which seems to suggest that the "reasonable expectation of privacy" test might be applied here, however it would be too soon to comment on that till the issue is brought before the Indian courts to fully explain the scope of the section.

Disclosure of Identity of a Rape Victim

Offense	Fine	Imprisonment
The disclosure of identity of victims of rape and related offenses.[17]	To be determined	Two years

[16] Indian Penal Code, 1860, section 354C.
[17] *Id*. section 228A.

Unnatural Offences

Offense	Fine	Imprisonment
Any individual who has carnal intercourse against the order of nature with any man, woman, or animal.[18]	Not specified	Extend to life or ten years

Omission of Documents

Offense	**Fine**	**Imprisonment**
Any individual who purposefully fails to produce a document or electronic record, when legally bound to do so to any public servant or of any public servant.[19]	**Extend to Rs. 500**	**Up to one month**

Furnishing False Information

Offense	**Fine**	**Imprisonment**
Any individual that is legally bound to furnish information to a public servant, furnishes false information.[20]	Extend to Rs. 1,000	Up to six months
Any individual who furnishes false information which is required for the purpose of preventing the commission of an offence, apprehension of an offender, imprisonment etc. [21]	Not specified	Up to two years

[18] *Id*. section 377.
[19] *Id*. section 175.
[20] *Id*. section 177.
[21] *Id*. section 177.

National Investigation Agency Act, 2008

This Act creates the National Investigation Agency and empowers it to investigate and prosecute offences that affect the sovereignty, security, and integrity of India, security of State, friendly relations with foreign states and offences under the Act enacted to implement international treaties, agreements, conventions and resolutions of the United Nations. The Act applies to the whole of India and to Indian citizens outside of India, to Government Officials, and to persons on ships and aircrafts registered in India.[22] The Act also gives the Central Government the power to constitute a special court to hear cases investigated by the NIA.[23] The Act establishes a special court empowered to take cognizance of any offence, without the accused being committed to it for trial, after receiving a complaint of facts that constitute such offence or upon a police report of such facts. [24]

- *Powers of the Agency*: the Agency is given all the powers, duties, privileges, and liabilities that police officers and officers in charge of a police station have in connection to the investigation of offences.[25] While investigating one offence, the Agency may also investigate any other offence that the accused is alleged to have committed.[26] This is relevant because police officers have wide powers as discussed in the Cr.P.C. chapter.
- *Proceedings held in Camera*: If the Special Court desires, with reasons recorded in writing, the proceedings of the court will be held in camera.[27]
- *Protection of witnesses*: If the Special Court is satisfied that the life of a witness is in danger, it may take measures to keep the identity and address of such witness secret.[28] Particular steps that will be taken include: the holding of proceedings at a place decided by the Special Court, the avoiding of the mention of the name and addresses of the witnesses, the issuing of directions for securing the identity and address of the witnesses are not disclosed, a decision that is in the public interest to order that all or any of the proceedings pending before the Court will not be published in any manner. [29]

National Security Act, 1980

This Act allows the government to order detention of people in order to prevent actions prejudicial to the defence of India. However since this Act only provides for detention and procedure for appealing the detention orders, etc. the principles of privacy are not applicable to this Act, except principles relating to security of the data.

---

22 National Intelligence Agency Act 1980 s. 1
23 National Intelligence Agency Act 1980 s.11
24 National Investigation Act 2008 s. 16
25 National Investigation Agency Act, 2008, s. 3(2).
26 National Investigation Act 2008 s.8
27 National Investigation Act 2008 s. 17 (1)
28 National Investigation Act 2008 s. 17(2)
29 National Investigation Act 2008 s. 17(3) (a-d)

Proposed Legislation

The Intelligence Services (Powers and Regulations) Bill, 2011[30]

This Bill was introduced in response to increasing concerns over the unregulated and often haphazard manner in which the nation's agencies such as the Research & Analysis Wing (RAW)[31], the Intelligence Bureau (IB)[32] and the National Technical Research Organisation (NTRO)[33] function. The Bill creates a legislative and regulatory framework for the functioning and coordination of the Intelligence Bureau, the Research and Analysis Wing, and the National Technical Research Organization. In doing so the Bill creates a Designated Authority responsible for the oversight of certain actions of these agencies and creates a Tribunal to receive and investigate individual complaints and issue compensation to aggrieved individuals. The Bill also establishes the National Intelligence and Security Oversight Committee as an oversight mechanism to these agencies, and puts in place an Intelligence Ombudsman responsible for ensuring coordination and function of organizations.[34] The Bill extends to the whole of India, all citizens of India who are outside of India, all persons in the Government, and any person on ships and aircrafts registered in India. Bringing further clarity as to the exact crimes that these agencies will be functionable for, the Bill defines 'National Security' and 'threats to National Security'. *National security includes the sovereignty, territorial integrity, economic stability, and upholding of the Constitution. A threat to National Security includes (a) domestic and international terrorist acts (b) espionage that is directed against the country or otherwise detrimental to the country (c) sabotage directed against the vital national infrastructure of the country, (d) organized crime directed against the country or otherwise detrimental to the security of the country (e) drug, arms, and human trafficking directed against the country or otherwise detrimental to the security of the country (f) illegal international proliferation of weapons of mass destruction as well as materials and tools required for production, (g) illegal trafficking of internationally controlled products and technologies, and (h) organized acts of violence against ethnic or religious groups.* [35] Aspects of the Bill that impact privacy include:

- **Powers**
    - **RAW**: The powers of RAW will be exercisable 'in the interests of National security, with particular reference to the defense, security strategic, economic and foreign policies of the Union of India and in aiding the neutralization of threats from external sources'[36].
    - **IB**: IB will be responsible for completing work for purposes of 'national security'

[30] Research assisted by Tarun Krishnakumar
31S.4 of the Intelligence Services (Powers and Regulations) Bill, 2011.
32Id. s. 4
33Id. s. 6
34Id. s. 16
[35]Id. s. 2(vii), (x)
36Id. s.3

in the context of internal conflict and provide protection against threats from espionage, and terrorist acts. The IB will be responsible for the collection and management of intelligence within the country, safeguarding the economic well being of the country, and acting in aid to the central and state police [37]

  - **NTRO**: NTRO will be responsible for monitoring and interfering with all forms of communications as it sees fit, to collect and provide intercepted material to other agencies, to provide advice and assistance in languages and cryptography to the armed forces and other organizations as specified by the Prime Minister.[38] NTROs will only carry out these functions in the interests of national security, the economic well being of the country, and for the prevention, detection, interdiction, or investigation of crimes as prescribed by the Prime Minster.[39]

- **Security of information:**
  - **RAW:** It will be the responsibility of the head of RAW to ensure that no information is disclosed except as necessary.[40]
  - **IB:** It will be the responsibility of the Director of the IB to ensure that collected information is disclosed except as necessary.[41]
  - **NRTO:** It will be the responsibility of the Chairman to ensure that collected information is not disclosed except when necessary or for ensuring the security, stability, and sovereignty of the country.[42]
- **Oversight:**
  - **RAW:** The day to day functioning's of RAW will be overseen by officers appointed by the Prime Minister of India, not below the rank of Secretary to the Government of India.[43]
  - **IB:** The day to day functioning's of the IB will be overseen by a Director who will be appointed by the Prime Minister.[44]
  - **NTRO:** The data to day functioning's of NTRO will be overseen by a Chairman who will be appointed by the Prime Minister.[45]
- **Accountability:**
  - **RAW**: The head of RAW must submit a bi-annual report on the workings of the organizations to the Prime Minister.[46]
  - **IB**: The Director of the IB must submit a bi-annual report on the workings of the organization to the Prime Minister.[47]
  - **NTRO**: The Chairman of NTRO will submit a bi-annual report on the workings of the organization to the Prime Minister.[48]
- **Warrants and authorizations:** Officers from these organizations seeking authorization

---

37Id. S. 4(2),(3)
[38] Id. s.6(2)
39Id. 6(3).
[40] Id. s. 3(3).
[41] Id. s. 5(2)
[42] Id.s. 7(2a)
[43] Id. s.3(3)
[44] Id. s. 5(1)
[45] Id. s. 7(1)
[46] Id. s. 3(5)
[47] Id. s. 5(3)
[48] Id. s. 7(3)

must comply with the following regime and prescribed safeguards:

- **Requirement for Warrant**: Entry is not allowed into any property or interference with any form of communication unless a warrant is obtained from the designated authority under the Bill, or by the Prime Minister[49]. The designated authority has the power to cancel a warrant if he/she sees fit.[50] The designated officer cannot be below the rank of Secretary to the Central Government. [51] Warrants granted in relation to terrorist acts can extend to actions that take place outside of India.[52]
- **Procedure and grounds for warrant**: Before a warrant is issued, the designated authority must be satisfied that:
    - the action is necessary
    - the objective of the action cannot be reasonably achieved by any other means
    - Adequate safeguards are in place to protect against disclosure of obtained information. Are in force with respect to the disclosure of information obtained.[53]
- **Time Limit**: Unless renewed, a warrant will expire after three months from being issued. For a warrant to be renewed, it must be approved by the designated officer and can only be renewed for another three months.[54]
- **Use of collected information**: If information is collected without a specific warrant, the agency is allowed to use the information only for the purposes of authorizing fresh warrants, which must be sought 48 hrs after obtaining the information.[55]

- **Oversight of the legislation:** The Bill establishes a body known as the National Intelligence and Security Oversight Committee constituted for the purposes of overseeing the carrying out of the Act.[56] Among other things the committee will submit an annual report to the Prime Minister containing information related to RAW, IB, and NTRO. If the Prime Minister, in consultation with the committee, feels that information found in the report would hinder any of the agencies from carrying out its functions, it can delete the information from the report.[57] The Act also appoints an ombudsman who has the responsibility of resolving internal grievances and suggesting administrative practices for the intelligence agencies. Through the ombudsman, aggrieved members of the agencies can seek remedy including compensation and reversal, if possible, of an action.[58]
- **Tribunal***:* The Bill also creates the National Intelligence Tribunal for the purpose of investigating complaints against RAW, IB, and NTRO. The Tribunal will have analogous powers to a Civil Court.[59] Aggrieved individuals can submit complaints to the Tribunal, who will subsequently investigate the complaint and issue remedy where necessary.

[49] Id. s. 8(1) and 9(1)(b)
[50] Id. s. 9(4)
[51] Id s. 8(1)
[52] Id s.8(3)
[53] Id. s. 8(2)
[54] Id. s. 9(2)
[55] Id. s 11(2) &(3)
[56] Id. s. 12(1)
[57] Id. s. 12(1)&(5)&(6)
[58] Id. 21
[59] Id. s. 31(5)

Remedies under the Act include orders for destruction of information held about a person by the agencies, compensation, quashing of an order or authorization, or instituting proceedings under relevant laws in force.[60] Any individual who does not agree with the decision by the Tribunal may appeal the decision in the Supreme Court within 90 days of the order. [61]

Central Bureaus of Investigation Bill (CBI), 2010

This Act was proposed with the objective of providing legal sanctity to the CBI under Article 246 of the Constitution of India, to create one unified Central Government Agency, and harmonize its powers and functions. [62] The Bill has become even more important in the context of the recent judgment of the Gauhati High Court which held the formation of the CBI as illegal (although this order has been stayed by the Supreme Court) as well as the comments made by the Supreme Court regarding the independence of the CBI in the coal allocation scam. The Bill extends to the whole of India, to citizens of India who are not in India, to persons in the service of the Government, and to persons on ships, and registered Indian aircrafts.[63] The Bill provides for oversight of the CBI by the Central Government, and the administration of the Bureau to be overseen by a Director appointed by the Central Government.[64] The Bill gives the CBI the duties to prevent, investigate, and prosecute offenses under seventy nine laws in force.[65] Aspects of the Act that relate to privacy include:

As per the Bill the CBI is only empowered to prevent, investigate and prosecute offences under orders from the Central Government.[66] The supervision of the CBI shall vest with the Central Government except in case of offences which are covered under the Prevention of Corruption Act, 1988 in which case it shall be under the superintendence of the Central Vigilance Commission.[67] Officers of the bureau will have analogous powers as an officer in charge of a police station including powers and provisions relating to registration, investigation, arrest, search, seizure, and filing of final reports in the Court.[68]

Case Law[69]

R.M Malkani v. State of Maharashtra,[70] (1972)

In this case, the Coroner of Bombay was convicted of corruption and extortion for taking money to give a dishonest report. One of the pieces of evidence relied upon to convict the accused was the tape recorded telephonic conversation between the accused and another individual. The case

[60] Id. s. 34
[61] Id. s 35
[62] *Preambl*e. The CBI Bill 2010.
[63] Section 1, The CBI Bill, 2010.
[64] Section 4&5. CBI Bill, 2010
[65] Section 7. Laws in force that contain offences the CBI is permitted to investigate are found in Schedule 1&2.
[66] Section 8, CBI Bill, 2010
[67] Section 4, CBI Bill, 2010
[68] Section 11. CBI Bill, 2010
[69] Research and writing completed by Priyale Prasad
[70] http://www.judis.nic.in/supremecourt/imgs1.aspx?filename=6708

dealt with the principle that in the Unites States is referred to as ‘fruit of the poisonous tree’. In this case taped telephonic conversation which was not obtained in accordance with the interception provision of the Telegraph Act was produced in evidence and relied upon by the Trial Court and High Court. This reliance on allegedly illegally obtained telephonic conversation was challenged before the Supreme Court, among other things, on the ground that attaching a tape recording machine to the telephone violated section 25(b) of the Telegraph Act which provides that anyone intending to intercept or to acquaint himself with the contents of any message damages, removes, tampers with or touches any battery, machinery. telegraph line, post or other thin whatever, being part of or used in or about any telegraph or in the working thereof he shall be punished with imprisonment for a term which may extend to three years, or with fine, or with both. The Court dealt with this argument saying that it there is no bar in admitting relevant contemporaneous evidence even if it is obtained illegally. It was then argued that recording the telephonic conversation without specific consent would be a violation of the right to privacy of an individual, the Court held:

> “It was said by counsel for the appellant that the tape recorded conversation was obtained by illegal means. The illegality was said to be contravention of section 25 of the Indian Telegraph Act. There is no violation of section 25 of the Telegraph Act in the facts and circumstances of the present case. There is warrant for proposition that even if, evidence is illegally obtained it is admissible. Over a century ago it was said in an English case where a constable searched the appellant illegally and found a quantity of offending article in his pocket that it would be a dangerous obstacle to the administration of justice if it were held, because evidence was obtained by illegal means, it could not be used against a party charged with an offence. See *Jones* v. *Owen*. The Judicial Committee in *Kuruma, Son of Kanju* v. *R.* dealt with the conviction of an accused of being in unlawful possession of ammunition which had been discovered in consequence of a search of his person by a police officer below the rank of those who were permitted to make such searches. The Judicial Committee held that the evidence was rightly admitted. The reason given was that if evidence was admissible it matters not how it was obtained. There is of course always a word of caution. It is that the Judge has a discretion to disallow evidence in a criminal case if the strict rules of admissibility would operate unfairly against the accused. That caution is the golden rule in criminal jurisprudence.
>
> It was said that the admissibility of the tape recorded evidence offended Articles 20(3) and 21 of the Constitution. The submission was that the manner of acquiring the tape recorded conversation was not procedure established by law and the appellant was incriminated. The appellant's conversation was voluntary. There was no compulsion. The attaching of the tape recording instrument was unknown to the appellant. That fact does not render the evidence of conversation inadmissible. The appellant's conversation was not extracted under duress or compulsion. If the conversation was recorded on the tape it was a mechanical contrivance to play the role of an eavesdropper. In *R. v. Leatham*, [1861] 8 Cox.C.C.498 it was said "It matters not how you get it if you steal it even, it would be admissible in evidence".. As long as it is not tainted by an inadmissible confession of guilt evidence even if it is illegally obtained is admissible. There is no scope for holding that the appellant was made to incriminate himself. At the time of the conversation there was no case against the appellant. He was not compelled to speak or

> confess. Article 21 was invoked by submitting that the privacy of the appellant's conversation was invaded. Article 21 contemplates procedure established by law with regard to deprivation of life or personal liberty. The telephonic conversation of an innocent citizen will be protected by Courts against wrongful or high handed interference by tapping the conversation. The protection is not for the guilty citizen against the efforts of the police to vindicate the law and prevent corruption of public servants. It must not be understood that the Courts will tolerate safeguards for the protection of the citizen to be imperiled by permitting the police to proceed by unlawful or irregular methods. In the present case there is no unlawful or irregular method in obtaining the tape recording of the conversation."

It may be of interest to some that in this case, the Court unsurprisingly chose to rely upon the precedent in the UK which allows for illegally obtained evidence rather than the contradictory precedent of the United States which does not admit evidence if it has been obtained illegally. The term unsurprising has been used since it was the general practice in that time, and still is to a large extent, to rely upon UK precedent rather than the precedent of any other country.

Case Highlights

- **Although conversation was recorded without the consent of the person, that would not prevent it from being admissible as evidence**
- **Illegally obtained evidence is admissible in court**
- **Telephonic conversation of an innocent citizen will be protected by Courts against wrongful or high handed interference by tapping the conversation**

State of Maharashtra v. *Bharat Shanti Lal Shah and others,*[71](2008)

The Maharashtra Control of Organized Crime Act, 1999 is applicable only in Maharashtra and Delhi and is used extensively to combat organized crime in Mumbai and Delhi. This legislation, like certain other state legislations,[72] has provisions for interception and safeguards for the same.[73] These provisions and their safeguards are similar to the directives laid down by the Supreme Court in *PUCL*'s case and incorporated in the Telegraph Rules.

The legislative competence of the state to enact these provisions was challenged in front of the Supreme Court in this case. The Supreme Court while deciding on the constitutional validity of the impugned sections, observed that though the interception of communications is an invasion of an individual's right to privacy, the right to privacy is not absolute, thus the court is required to see that the procedure itself is fair, just, and reasonable. In the case, the Court held:

> "44. The interception of conversation though constitutes an invasion of an individual right to privacy but the said right can be curtailed in accordance to procedure validly established by law. Thus what the Court is required to see is that the procedure itself must be fair, just and reasonable and non arbitrary, fanciful or oppressive.

[71] http://www.judis.nic.in/supremecourt/imgs1.aspx?filename=32371
[72] Such as the Andhra Pradesh Control of Organised Crime Act, 2001, the Prevention of Terrorism Act, 2002 (now repealed), etc.
[73] Sections 13 – 16.

45. The object of the MCOCA is to prevent the organised crime, and a perusal of the provisions of Act under challenge would indicate that the said law authorizes the interception of wire, electronic or oral communication only if it is intended to prevent the commission of an organised crime or if it is intended to collect the evidence to the commission of such an organized crime. The procedures authorizing such interception are also provided therein with enough procedural safeguards, some of which are indicated and discussed hereinbefore. In addition under Section 16 of the MCOCA, provision for prohibiting and punishing the unauthorized use of information acquired by interception of wire, electronic or oral communication has been made. Thus as the Act under challenge contains sufficient safeguards and also satisfies the aforementioned mandate the contention of the respondents that provisions of Section 13 to 16 are violative of the Article 21 of the Constitution cannot also be accepted."

Case Highlights

- Interception of conversation is an invasion of the right to privacy but the right can be curtailed through a procedure established by law
- Court is required to see is that the procedure itself must be fair, just and reasonable and non arbitrary, fanciful or oppressive
- The MCOCA contains sufficient safeguards and also provides for punishment for unauthorized use of information acquired by interception and therefore is not violative of Article 21 of the Constitution. The Court thus seems to indicate that the MCOCA contains provisions regarding purpose limitation.

State (N.C.T. of Delhi) v. *Navjot Sandhu @ Afsan Guru*[74] (*Afsan Guru case*), (2005)

Since there is not much case law under the present anti terror law which is the Unlawful Activities (Prevention) Act, 1967 we shall discuss a case under the previous anti terror law, the Prevention of Terrorism Act, 2002 (now repealed) in the famous Parliament attack case also known as *State (N.C.T. of Delhi)* v. *Navjot Sandhu @ Afsan Guru*[75] (*Afsan Guru case*) where several armed gunmen stormed the Indian Parliament complex. Navjot Sandhu @ Afsan Guru was accused and convicted of being involved in the conspiracy to carry out the attack. The Supreme Court of India, in this case had to determine the admissibility of information obtained through unauthorized interception and held as follows:

"The legality and admissibility of intercepted telephone calls arises in the context of telephone conversation between Shaukat and his wife Afsan Guru on 14th December at 20:09 hrs and the conversation between Gilani and his brother Shah Faizal on the same day at 12:22 hrs. Interception of communication is provided for by the provisions contained in Chapter V of the POTO/POTA which contains Sections 36 to 48. The proviso to Section 45 lays down the pre-requisite conditions for admitting the evidence collected against the accused through the interception of wire, electronic or oral communication. Chapter V governing the procedure for interception and admission of the intercepted communications pre-supposes that there is an

[74] http://www.judis.nic.in/supremecourt/imgs1.aspx?filename=27092
[75] http://www.judis.nic.in/supremecourt/imgs1.aspx?filename=27092

investigation of a terrorists act under the POTA has been set in motion. It is not in dispute that the procedural requirements of Chapter V have not been complied with when such interceptions took place on 14th December, 2001. But, as already noticed, on the crucial date on which interception took place (i.e. 14th December), no offence under POTA was included whether in the FIR or in any other contemporaneous documents. We have already held that the non-inclusion of POTO offences even at the threshold of investigation cannot be legally faulted and that such non-inclusion was not deliberate. The admissibility or the evidentiary status of the two intercepted conversations should, therefore, be judged de hors the provisions of POTO/POTA. On the relevant day, the interception of messages was governed by Section 5(2) of the Indian Telegraph Act read with Rule 419-A of the Indian Telegraph Rules. The substantive power of interception by the Government or the authorized officer is conferred by Section 5. The modalities and procedure for interception is governed by the said Rules. It is contended by the learned senior counsel appearing for the two accused Shaukat and Gilani, that even the Rule 419A, has not been complied with in the instant case, and, therefore, the tape- recorded conversation obtained by such interception cannot be utilized by the prosecution to incriminate the said accused. It is the contention of learned counsel for the State, Mr. Gopal Subramanium, that there was substantial compliance with Rule 419A and, in any case, even if the interception did not take place in strict conformity with the Rule, that does not affect the admissibility of the communications so recorded. In other words, his submission is that the illegality or irregularity in interception does not affect its admissibility in evidence there being no specific embargo against the admissibility in the Telegraph Act or in the Rules. Irrespective of the merit in the first contention of Mr. Gopal Subramanium, we find force in the alternative contention advanced by him."

It is interesting to note that draconian as the Prevention of Terrorism Act, 2002 may have been,[76] its provisions for interception of communications seem to have been very well thought out and incorporated a number of safeguards, specially section 45 and 46 (4) which said that interception was not admissible unless the accused is given a copy of the order approving the interception, thus making illegal interceptions inadmissible. Therefore unless the interception order itself was obtained by fraud, this provision provided an excellent safeguard against the use of illegally obtained interceptions for evidentiary purposes, sort of neutralizing the ratio of *R.M. Malkani's case*. The Prevention of Terrorism Act, 2002 also had admissibility and notice safeguards as well as the probable cause standard incorporated into its interception provisions. These safeguards are not present either in the Telegraph Act, 1885 or the Information Technology Act, 2000 but the provision requiring provision of the interception order before producing it in evidence is present in the Unlawful Activities Prevention Act, 1967.

Case Highlights

- **The pre-requisite conditions under POTA for admitting the evidence collected against the accused through the interception of wire, electronic or oral communication have to be complied with before accepting such material in evidence.**

[76] The Act allowed for a confession made in front of police officers to be used as evidence and allowed for an accused to be detained for extended periods of time without being produced before a Magistrate, etc.

Selvi v. State of Karnataka,[77] (2010)

In 2010, *Smt. Selvi Ors. v. State of Karnataka*, the Supreme Court of India gave a comprehensive judgment on the validity and constitutionality of various scientific techniques such as brain mapping and narco analysis. The Court looked at the issue of reliability/unreliability of the tests and also acknowledged that such procedures do raise concerns of privacy violation, both mental privacy as well as physical. While discussing this issue the Court held:

> "169. There are several ways in which the involuntary administration of either of the impugned tests could be viewed as a restraint on `personal liberty'. The most obvious indicator of restraint is the use of physical force to ensure that an unwilling person is confined to the premises where the tests are to be conducted. Furthermore, the drug-induced revelations or the substantive inferences drawn from the measurement of the subject's physiological responses can be described as an intrusion into the subject's mental privacy. It is also quite conceivable that a person could make an incriminating statement on being threatened with the prospective administration of any of these techniques. Conversely, a person who has been forcibly subjected to these techniques could be confronted with the results in a subsequent interrogation, thereby eliciting incriminating statements…..
>
> 191. Moreover, a distinction must be made between the character of restraints placed on the right to privacy. While the ordinary exercise of police powers contemplates restraints of a physical nature such as the extraction of bodily substances and the use of reasonable force for subjecting a person to a medical examination, it is not viable to extend these police powers to the forcible extraction of testimonial responses. In conceptualising the `right to privacy' we must highlight the distinction between privacy in a physical sense and the privacy of one's mental processes.
>
> 192. So far, the judicial understanding of privacy in our country has mostly stressed on the protection of the body and physical spaces from intrusive actions by the State. While the scheme of criminal procedure as well as evidence law mandates interference with physical privacy through statutory provisions that enable arrest, detention, search and seizure among others, the same cannot be the basis for compelling a person `to impart personal knowledge about a relevant fact'. The theory of interrelationship of rights mandates that the right against self-incrimination should also be read as a component of `personal liberty' under Article 21. Hence, our understanding of the `right to privacy' should account for its intersection with Article 20(3). Furthermore, the `rule against involuntary confessions' as embodied in Sections 24, 25, 26 and 27 of the Evidence Act, 1872 seeks to serve both the objectives of reliability as well as voluntariness of testimony given in a custodial setting. A conjunctive reading of Articles 20(3) and 21 of the Constitution along with the principles of evidence law leads us to a clear answer. We must recognise the importance of personal autonomy in aspects such as the choice between remaining silent and speaking. An individual's decision to make a statement is the product of a private choice and there should be no scope for any other individual to

[77] http://www.judis.nic.in/supremecourt/imgs1.aspx?filename=36303

interfere with such autonomy, especially in circumstances where the person faces exposure to criminal charges or penalties.

193. Therefore, it is our considered opinion that subjecting a person to the impugned techniques in an involuntary manner violates the prescribed boundaries of privacy. Forcible interference with a person's mental processes is not provided for under any statute and it most certainly comes into conflict with the `right against self-incrimination'. However, this determination does not account for circumstances where a person could be subjected to any of the impugned tests but not exposed to criminal charges and the possibility of conviction. In such cases, he/she could still face adverse consequences such as custodial abuse, surveillance, undue harassment and social stigma among others. In order to address such circumstances, it is important to examine some other dimensions of Article 21."

Thus the court found that brain mapping, polygraph and narco analysis violated individuals' right to privacy by intruding into a "subject's mental privacy," denying an opportunity to choose whether to speak or remain silent, and physically restraining a subject to the location of the tests and amounted to cruel, inhuman or degrading treatment.

Case Highlights

- The Court acknowledged the distinction between bodily/physical privacy and mental privacy
- The scheme of criminal and evidence law mandates interference with the right to physical and bodily privacy in certain circumstances, but the same cannot be used to compel a person `to impart personal knowledge about a relevant fact'
- This case also establishes the intersection of the right to privacy with Article 20(3)
- An individual's decision to make a statement is the product of a private choice and there should be no scope for any other individual to interfere with such autonomy
- Subjecting a person to techniques such as narcoanalysis, polygraph examination and the Brain Electrical Activation Profile (BEAP) test without consent violates the subject's mental privacy

Implementation

Indian Intelligence Agencies

Indian Intelligence today comprises of various Central as well as State agencies. All Central agencies can be grouped under three ministries: The Ministry of Defense, Ministry of State for Home Affairs, and the Ministry of Finance. At the top of the intelligence organizations in India is the Joint Intelligence Committee (JIC). Within the JIC is the National Security Council (NSC), which includes as its members, the Home Minister, Minister of External Affairs, Minister of

Defense, and the Finance Minister. After the JIC is the Research and Analysis Wing (RAW), and the Intelligence Bureau (IB).[78] These various agencies at the Central as well as the State level are given the power to intercept communications based upon "well reasoned" orders. According to a 2011 Government Notification, RAW became one of the eight agencies empowered to intercept phone calls, email, and voice and data communications 'domestically'. The other agencies are the Intelligence Bureau, Directorate of Revenue Intelligence, Enforcement Directorate, Narcotics Control Bureau, Central Bureau of Investigation, National Technical Research Organization, and State police.[79] The functioning's of these organizations are for the most part, a black box to the public, though the Right to Information Act requires that all agencies and governmental bodies must reveal information that they have pertaining human rights violations and corruption cases registered against its officials. [80]

NATGRID

In 2011, the National Intelligence Grid (NATGRID) was established as an attached office of the Ministry of Home Affairs, and facilitates monitoring by giving security agencies a license to go through and link sources of information - such as an individual's tax, travel, internet, and telecom usage information. The database was created in response to the Mumbai terrorist attacks, and is hoped to help counter terrorism by acting as a tool only for security agencies to use specifically when locating and obtaining relevant information about a terrorist. Many citizens and Indian Ministries have raised concerns that the project will facilitate tracking and has a number of privacy implications. NATGRID maintains that privacy is not implicated as it is only a technical interface for intelligence agencies – and not an organization. Currently there are eleven structural and procedural safeguards and oversight mechanisms in place to ensure that the system is not misused. [81] To head the project, the then Union Home Minister P. Chidambaram appointed Raghu Menon, a private sector security expert, as chief executive officer of NATGRID.82 Implementation of the NATGRID scheme has been envisioned in four phases. The first two phases have been approved by the Cabinet Committee on Security (CCS) and deal with the centralized storage and sharing of data which can be legally accessed by the law enforcement agencies. The CCS has also given assent to the next two phases 'in principle'. However, the next two phases raise grave privacy concerns as they deal with property details, bank transaction records, internet usages etc. The CCS has said that there will most likely be amendments to the existing laws to implement the next two phases.83

---

[78] Ibid http://www.defencejournal.com/sept99/analysis.html

[79] RAW gets power to tap phones, track emails, The Times of India, Dec. 19, 2011, available at http://articles.timesofindia.indiatimes.com/2011-12-19/india/30533559_1_national-technical-research-organisation-agencies-intercept

[80] RTI Act section 24

81 Agarwal, V. (2011) Q&A: NATGRID Chief Raghu Raman. The Wall Street Journal. June 29th. Accessed January 2012. Available at: http://blogs.wsj.com/indiarealtime/2011/06/29/qa-natgrid-chief-raghu-raman/

82 Aloke Tikku & Gaurav Choudhury, Database to fight terrorism will keep eye on you, Hindustan Times, Dec. 23, 2009, available at http://www.hindustantimes.com/News-Feed/india/Database-to-fightterrorism-will-keep-eye-on-you/Article1-489540.aspx (last visited on Jan. 25, 2012)

83 Vishwa Mohan, NATGRID to show its first result in 18 months, The Times of India, June 8, 2011, available at http://articles.timesofindia.indiatimes.com/2011-06-08/india/29633448_1_phases-natgrid-data (last visited on Jan. 25, 2012)

Crime and Criminal Tracking Network & Systems

Developed by the Ministry of Home Affairs, and taken forward by the National Crime Records Bureau, the CCTNS aims to create a nation-wide networked infrastructure for the evolution of an IT-enabled criminal tracking system. The project envisions connectivity between police units within the States and Union Territories as well as linking police functions at State and Central levels to external entities. Once implemented, the CCTNS will link the State Crime Records Bureau with the National Crime Record Bureau, thus creating a database that can be accessed in real-time from any police station across the country. The goals of the system are to facilitate collection, storage, retrieval, analysis, transfer and sharing of data and information at the police station and between the police station and the State Headquarters and the Central Police Organizations. The system will migrate data that is no older than ten years.[84] In the CCTNS database, law enforcement can search for cases using the following filters: FIR No, Date Range, Beat Area, Time Interval, Type of Case. Advanced searches in the system allow law enforcement to search based on: type of crime, accused details, criminal detail, suspect detail, and victim details.[85] The CCTNS looks to replace the many policing initiatives that exist today and create an accessible and connected platform. Some of the past policing initiatives include programs such as the NCRB-led CCIS (Crime and Criminals Information System) and CIPA (Common Integrated Police Application), and State-led initiatives such as e-COPS (in Andhra Pradesh), Police IT (in Karnataka), Thana Tracking System (in West Bengal), CAARUS (in Tamil Nadu) and HD IITS (in Gujarat). [86]

CCTV[87]

In India there is no particular regulatory authority or government department that is designated to look into any abuse or misuse of CCTV. The largest uses of the CCTV for surveillance have been in the metro cities of India, such as a Delhi, Mumbai, Chennai, and Bangalore.[88] This does not rule out the usage of CCTV in towns other than metros, but the technology has yet to become rampant in small towns and villages. Thus, in India there is a connection between the use of CCTV surveillance and urbanisation. CCTV technology is perceived to be necessary for both the security and development element by the state.[89] Furthermore, CCTV is used to bring in transparency in the government offices and also for deterrence among students.[90] As per the news

---

84 Ministry of home Affairs. (2009). Union Home Minister's mission statement for NCRB under CCTNS. December 23rd. Accessed December 2011. Available At: http://ncrb.nic.in/cctns.htm

85 Ministry of Home Affairs. Crime & Criminal Tracking Network and Systems (CCTNS): Search Module. GOI. Available at: http://ncrb.nic.in/04%20Search%20Module_v1.1.pdf

86 Government of Goa. Criminal & Criminal Tracking Network & Systems (CCTNS) Implementation of CCTN in GOA. Available at: http://ncrb.nic.in/All%20State%20RFP/Goa/Volume%20III.pdf

87 Research completed by Deva Prasad and Suchritra Menon

88 Please see http://www.hindu.com/2010/07/12/stories/2010071258290300.htm, (Last accessed on 12.03.2011),http://www.siliconindia.com/shownews/India_to_setup_CCTV_in_crowded_places-nid-67718.html (Last accessed on 12.03.2011)

89Seehttp://timesofindia.indiatimeshttp://www.nyxsecurity.com/pages/about-nyx/why-the-legislation/.com/city/pune/CCTV-cameras-in-public-places-will-need-govts-go-ahead/articleshow/7455826.cms (Last accessed on 12.03.2011)

90Ibid, also see http://ibnlive.in.com/news/blore-officer-hooks-cctv-to-official-website/142465-3.html (Last accessed on 12.03.2011)

report, Pune Municipal Corporation (PMC) has planned to implement round the clock CCTV surveillance at all public places so as to increase the security measures following a bomb blast at a bakery in the city which had taken the life of seventeen persons. The PMC has proposed to the Maharashtra state government an amendment in the Development Control Rules applicable to the PMC as it is governed by the Bombay Provincial Municipal Corporations Act, 1949, which is a state legislation. An amendment would allow the PMC to make it mandatory for the shopping malls, markets, religious structures, hotels, important tourist attractions, exclusive business buildings, historical buildings and the offices of government and semi-government organisations to install CCTV's. [91]

National Security Database
http://www.indianexpress.com/news/ntro-on-board-cyber-security-database-coming/880721/

91Ibidhttp://timesofindia.indiatimeshttp://www.nyxsecurity.com/pages/about-nyx/why-the-legislation/.com/city/pune/CCTV-cameras-in-public-places-will-need-govts-go-ahead/articleshow/7455826.cms (Last accessed on 12.03.2011)