State of Cyber Security and Surveillance in India

A Review of the Legal Landscape

Introduction

The issue of cyber security and surveillance, especially unauthorised surveillance, though traditionally unprioritised, has recently gained much traction due to the increasing number of news reports regarding various instances of unauthorised surveillance and cyber crimes. In the case of unauthorised surveillance, more than the frequency of the instances, it is their sheer magnitude that has shocked civil society and especially civil rights groups. In the background of this ever increasing concern regarding surveillance as well as increasing concerns regarding cyber security due to the increased pervasiveness of technology in our society, this paper tries to discuss the legal and regulatory landscape regarding surveillance as well as cyber security. The paper starts with an overview of the right to privacy, which forms one of the fundamental elements of any challenge to illegal surveillance. It then discusses the legal provisions dealing with interception under the two main legislations utilised for surveillance as well as some of the minor statutes, and tries to highlight the conditions imposed and incorporated into the law to avoid unauthorised interception. The paper then discusses the provisions relevant to interception and surveillance incorporated in the License Agreements for Internet Service Providers (ISPs), Telecom Service Providers (TSPs) as well as the Unified Access Service (UAS) License. It then discusses the major provisions dealing with cyber security by elaborating on the relevant provisions in the Information Technology Act, 2000 as well as the Rules framed under it before exploring the connect between privacy and transparency and dealing with the provisions of the Right to Information Act, 2005 insofar as they are relevant to this discussion. The paper then moves to a discussion of the major regulatory authorities dealing with Surveillance as well as Cyber Security before finally discussing the issues dealing with the digital evidence, its evidentiary value and how to present the same in a Court of law.

Legal Landscape for Privacy

India is a signatory to the Universal Declaration on Human Rights (Article 12) and the International Convention on Civil and Political Rights (Article 17) – both of which recognize privacy as a fundamental right. Though a member and signatory of these conventions, India does not have laws which guarantee a right to privacy to its citizens. In order to fill this lacuna in the law, the Courts in India have tried to enforce a right to privacy in favour of its citizens through two main routes, *viz*. a recognition of a constitutional right to privacy which has been read as part of the rights to life and personal liberty as well as the freedom of

expression and movement guaranteed under the Constitution; and a common law right to privacy which is available under tort law and has been borrowed primarily from American jurisprudence. It must be mentioned at the outset that the privacy is not a very strongly enforced right in India and there are a number of exceptions to the right to privacy which have been carved out by the Courts over a period of time, which we shall discuss later in this section.

The right to privacy was recognised as a constitutional principle in India for the first time by the Supreme Court in 1962 in the case of *Kharak Singh* v. *Union of India*,[1] in the background of the right of the police to physically keep checks on people who are repeat offenders (also known as history-sheeters). Although a majority of three Judges in the case categorically denied the existence of a constitutional right to privacy as part of the right to life and personal liberty,[2] two Judges disagreed with this analysis and held that

> "…the right to personal liberty takes in not only a right to be free from restrictions placed on his movements, but also free from encroachments on his private life. It is true our Constitution does not expressly declare a right to privacy as a fundamental right, but the said right is an essential ingredient of personal liberty."

Later in the case of *Govind* v. *State of M.P.*,[3] the Supreme Court in a similar factual background endorsed the view taken by the minority in *Kharak Singh*[4] and the right to privacy in India has become understood as an entrenched constitutional right under Indian law. In this case the Supreme Court discussed the right to privacy at length and debated the scope of and exceptions to this right as well. After discussing the scope of the right in the Indian context, the Court came to the conclusion that the right to privacy is not an absolute right and laid down three different tests which can be used to determine whether the right to privacy would be upheld/enforced in a given situation or not. These three tests are: (i) important countervailing interest which is superior, (ii) compelling state interest test, and (iii) compelling public interest. However, the Court later used phrases such as "reasonable restriction in public interest" and "reasonable restriction upon it for compelling interest of State" interchangeably which seems to suggest that the terms "compelling public interest" and "compelling state interest" used by the Court were being used synonymously and the Court does not draw any distinction between them. It is also important to note that the wider phrase "countervailing interest is shown to be superior" seems to suggest that it is possible, at least in theory, to have other interests apart from public interest or state interest also which could trump the right to privacy.

After the case of *Govind* v. *State of M.P.*,[5] the right to privacy was firmly established as a fundamental right guaranteed to the citizens of India, but with a limited scope and a number of exceptions. We could discuss all the judgements that have sculpted the constitutional jurisprudence on privacy in Indian law, but for the sake of brevity and to avoid repetition we will just summarize the ratio from those cases in a few bullet points:

a) Reasonable restrictions can be imposed on the right to privacy in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with

---

1 http://www.judis.nic.in/supremecourt/imgs1.aspx?filename=3641.

2 Article 21 of the Constitution of India, 1950. However in the later case of *PUCL v. Union of India* (discussed later), the Supreme Court insisted that all seven Judges had interpreted Article 21 to include the right to privacy.

3 http://www.judis.nic.in/supremecourt/imgs1.aspx?filename=6014.

4 http://www.judis.nic.in/supremecourt/imgs1.aspx?filename=3641.

5 http://www.judis.nic.in/supremecourt/imgs1.aspx?filename=6014.

foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence;[6]

b) Reasonable restrictions can be imposed upon the right to privacy either in the interests of the general public or for the protection of the interests of any Scheduled Tribe;[7]

c) The right to privacy can be restricted by procedure established by law which procedure would have to satisfy the test laid down in the *Maneka Gandhi case*.[8]

d) The right can be restricted if there is an important countervailing interest which is superior;[9]

e) It can be restricted if there is a compelling state interest to be served by doing so;[10]

f) It can be restricted in case there is a compelling public interest to be served by doing so;[11]

g) The *Rajagopal tests* - This case lays down three exceptions to the rule that a person's private information cannot be published, *viz.* i) person voluntarily thrusts himself into controversy or voluntarily raises or invites a controversy, ii) if publication is based on public records other than for sexual assault, kidnap and abduction, iii) there is no right to privacy for public officials with respect to their acts and conduct relevant to the discharge of their official duties. It must be noted that although the Court talks about public records, it does not use the term 'public domain' and thus it is possible that even if a document has been leaked in the public domain and is freely available, if it is not a matter of public record, the right to privacy can still be claimed in regard to it.[12]

The scope and exceptions to the right to privacy both have developed over the years in various contexts through various cases which have laid down the scope of the right to privacy in specific fields, which we shall discuss below so as to give a brief overview of the privacy landscape in Indian laws.

Freedom of the Press

It is pretty obvious to anyone at first glance that the right to privacy would share a complicated relationship with the freedom of the press, which is protected by the

---

6 Article 19(2) of the Constitution of India, 1950.

7 Article 19(5) of the Constitution of India, 1950.

8 *Maneka Gandhi* v. *Union of India*, Supreme Court of India, WP No. 231 of 1977, dated 25-01-1978. The test laid down in this case is universally considered to be that the procedure established by law which restricts the fundamental right should be just, fair and reasonable.

9 *Govind* v. *State of M.P.*, Supreme Court of India, WP No. 72 of 1970, dated 18-03-1975.

10 *Govind* v. *State of M.P.*, Supreme Court of India, WP No. 72 of 1970, dated 18-03-1975.

11 *Govind* v. *State of M.P.*, Supreme Court of India, WP No. 72 of 1970, dated 18-03-1975. However the Court later used phrases such as "reasonable restriction in public interest" and "reasonable restriction upon it for compelling interest of State" interchangeably which seems to suggest that the terms "compelling public interest" and "compelling state interest" used by the Court are being used synonymously and the Court does not draw any distinction between them. It is also important to note that the wider phrase "countervailing interest is shown to be superior" seems to suggest that it is possible, at least in theory, to have other interests apart from public interest or state interest also which could trump the right to privacy.

12 *R. Rajagopal v. Union of India*, Supreme Court of India, dated 7-10-1994. These tests have been listed as one group since they are all applicable in the specific context of publication of private information.

fundamental right of freedom of expression. In India there is an institution called the Press Council of India which is a mechanism for the Press to regulate itself. The Press Council of India issues various Norms and Guidelines which address some of the thorny issues of journalistic conduct including the right to privacy of the subjects of their reporting. It must be noted that some of the principles enunciated in these guidelines have been adopted from those propounded by the Courts while discussing the issue of privacy and freedom of the Press. Although the guidelines do specifically regulate some of the areas of journalistic conduct regarding the privacy of the subjects, however these guidelines are not legally enforceable and therefore lack any a strong enough mechanism to ensure their compliance.

The guidelines state that "The Press shall not intrude or invade the privacy of an individual, unless outweighed by genuine overriding public interest, not being a prurient or morbid curiosity. So, however, that once a matter becomes a matter of public record, the right to privacy no longer subsists and it becomes a legitimate subject for comment by the Press and the media, among others. Special caution is essential in reports likely to stigmatise women."[13] The guidelines make a distinction between the degree of privacy to be enjoyed by different people and under different circumstances, i.e. a representative or emissary of the public is not afforded the same degree of privacy as a private person. The guidelines also caution against identification of victims of sexual abuse, children of forcible marriages or illicit sexual unions, etc. They also ask journalists not to intrude into moments of personal grief of individuals.[14]

Other than these guidelines by the Press Council of India, the only legislation of some impact which affects the issue of privacy and the media is the Juvenile Justice (Care and Protection) of Children Act, 2000 which makes it an offence for the media to disclose the names, addresses or schools, or pictures of juveniles who are involved in a legal proceeding under the Act which would lead to their identification.[15]

The issue of freedom of the press and privacy was discussed at length in the case of *R. Rajagopal v. Union of India*,[16] (also known as the *Auto Shanker case*) where certain public officials approached the Supreme Court to stop the publication of an autobiography of a convict which contained embarrassing allegations regarding their dealings with the convict. It was argued that allowing the publication of these details/allegations would amount to a breach the right to privacy of these public officials. After a detailed discussion of the scope of the right to privacy, the Court agreed with the principle that a person's private information cannot be published but laid down three exceptions to this rule, *viz.* i) person voluntarily thrusts himself into controversy or voluntarily raises or invites a controversy, ii) if publication is based on public records other than for sexual assault, kidnap and abduction, iii) there is no right to privacy for public officials with respect to their acts and conduct relevant to the discharge of their official duties. It must be noted that although the Court talks about public records, it does not use the term 'public domain' and thus it is possible that even if a document has been leaked in the public domain and is freely available, if it is not a matter of public record, the right to privacy can still be claimed in regard to it.

The above stated principles were further clarified in the case of *Indu Jain* v. *Forbes Incorporated*,[17] where a case was filed by Indu Jain in the Delhi High Court to stop Forbes

---

13 Principles and Ethics for Journalists, Press Council of India, http://presscouncil.nic.in/Content/62_1_PrinciplesEthics.aspx.

14 Principles and Ethics for Journalists, Press Council of India, http://presscouncil.nic.in/Content/62_1_PrinciplesEthics.aspx.

15 Section 21, Juvenile Justice (Care and Protection of Children) Act, 2000.

16 http://www.judis.nic.in/supremecourt/imgs1.aspx?filename=11212

17 http://lobis.nic.in/dhc/GM/judgement/25-01-2010/GM12102007S21722006.pdf

magazine from featuring her family in the Forbes List of Indian Billionaires. After a discussion of the various authorities and cases on the issue the Court further clarified the principles relating to privacy and freedom of the press which are summarized below:

- In evaluating a relief to be granted in respect of a complaint against infraction of the right to privacy, the court has to balance the rights of the persons complaining of infraction of right to privacy against freedom of press and the right of public to disclosure of newsworthy information. Such consideration may entail the interest of the community and the court has to balance the proportionality of interfering with one right against the proportionality of impact by infraction of the other.
- Since public figures like public officials play an influential role in ordering society the citizen has a legitimate and substantial interest in the conduct of such persons and the freedom of press extends to engaging in uninhibited debate about the involvement of public figures in public issues and events.
- A public person or personage is one who by his standing, accomplishment, fame, mode of life or by adopting a profession or calling which gives the public a legitimate interest in his doings, affairs and character has so become a public figure and thereby relinquishes at least a part of his privacy.
- Public or general interest in the matter published has to be more than mere idle curiosity for it to be an exception to the right to privacy.
- The standard to be adopted for assessing as to whether the published material infracts the right to privacy of any individual is that of an ordinary man of common sense and prudence and not an out of ordinary or hyper-sensitive man.
- The publication has to be judged as a whole and news items, advertisements and published matter cannot be read without the accompanying message that is purported to be conveyed to public. Pre-publication censorship may not be countenanced in the scheme of the constitutional framework unless it is established that the publication has been made with reckless disregard for truth, publication shall not be normally prohibited.

Medical Privacy

Confidentiality and privacy are essential to all trusting relationships, such as that between patients and doctors. Moreover, in a healthcare context, patient confidentiality and the protection of privacy is the foundation of the doctor-patient relationship. Patients must feel comfortable sharing private information about their bodily functions, physical and sexual activities, and medical history. In areas where there exists a traditionally strong jurisprudence of confidentiality, such as health, finance, etc. Indian law follows the English common law principles of confidentiality which generally requires three elements to succeed, apart from contract, (i) the information itself must have the necessary quality of confidence about it, (ii) that information must have been imparted in circumstances importing an obligation of confidence, and (iii) there must be an unauthorized use of that information to the detriment of the party communicating it.[18]

The medical profession in India is regulated and overseen by the Medical Council of India (**MCI**) which issues certain regulations from time to time to regulate the conduct of the medical professionals in India. The MCI's Code of Ethics Regulations, 2002 impose a duty on physicians to protect the confidentiality of patients including their personal and domestic lives, unless the law requires their revelation, or if there is a serious and identified risk to a specific person and / or community or notifiable disease.[19] Similarly the Ethical Guidelines

---

18 *Coco* v. *A.N Clark (Engineers) Ltd.,* [1969] RPC 41 (UK).

19 *Code of Ethics Regulations,* 2002 Chapter 7, Section 7.14.

for Biomedical Research on Human Subjects released by the Indian Council for Medical Research in 2006 contain specific provisions relating to privacy of the research subjects.[20]

Apart from the above regulations there have been a few important cases in the field of medical privacy which have further tried to clarify the scope of the right to privacy in the medical and health sector. The first really important case in this field was *Mr. X v. Hospital Z, Supreme Court of India,*[21] where the Supreme Court had to strike a balance between a patients's right to privacy vis-a-vis the health and well being of third parties who may be at risk by coming into contact with the patient. The facts of this case were very interesting, a person who was engaged to be married was found to be HIV positive. This information was released by the doctor to the petitioner's family and through them to the family of his fiancée without the consent of the patient. The Supreme Court in this case held that a person could not invoke his "right to privacy" to prevent a doctor from disclosing his HIV-positive status to others. It was ruled that in respect of HIV-positive persons, the duty of confidentiality between the doctor and patient could be compromised in order to protect the health of other individuals. The Court held that in such a case disclosure by the Doctor could not be violative of either the rule of confidentiality or the patient's right of privacy as the person with whom the patient was likely to be married was saved in time by such disclosure. The Court held that:

> "26. Right of Privacy may, apart from contract, also arise out of a particular specific relationship which may be commercial, matrimonial, or even political. As already discussed above, Doctor-patient relationship, though basically commercial, is, professionally, a matter of confidence and, therefore. Doctors are morally and ethically bound to maintain confidentiality. In such a situation, public disclosure of even true private facts may amount to an invasion of the Right of Privacy which may sometimes lead to the clash of person's "right to be let alone" with another person's right to be informed.
>
> 28. Having regard to the fact that the appellant was found to be HIV(+), its disclosure would not be violative of either the rule of confidentiality or the appellant's Right of Privacy as Ms. Akali with whom the appellant was likely to be married was saved in time by such disclosure, or else, she too would have been infected with the dreadful disease if marriage had taken place and consummated."

Expanding the logic of this case further, it could be argued that this principle of disclosure to the person at risk could be applicable to other communicable and life threatening diseases as well, while a conservative opinion would be that this principle should only be applied to HIV+ cases. It may also be noted that the Court in this case did not discuss whether disclosure of such a disease may be made to only the persons at risk or to the public in general, although it would be safe to say that since most cases as well as medical ethics require the doctors to keep the patient's health records private, it is highly unlikely that 'disclosure' can be made to the public in general.

The other landmark decision in the realm of medical privacy is the case of *Sharda* v. *Dharmpal,*[22] where the basic question was whether a party to a divorce proceeding can be compelled to a medical examination. The wife in the divorce proceeding refused to submit herself to medical examination to determine whether she was of unsound mind on the ground that such an act would violate her right to personal liberty. Discussing the balance

---

[20] Ethical Guidelines for Biomedical Research *on* Human Subjects. (2006) Indian Council of Medical Research New Delhi.

[21] http://www.judis.nic.in/supremecourt/imgst.aspx?filename=19994

[22] http://www.judis.nic.in/supremecourt/imgs1.aspx?filename=19039

between protecting the right to privacy and other principles that may be involved in matrimonial cases such as the 'best interest of the child' in case child custody is also in issue, the Court held:

> "75. If the nature of the information relates directly to the well-being of the child or to the parent's ability to adequately care for child, and the court believes the child is potentially in danger, courts are likely to admit the information despite a patient's expectation of confidentiality. There are two competing interests involved when a court determines whether to compel discovery of a patient-litigant's mental health records over his objection in a child custody dispute. The first involves the privacy, confidentiality and privilege expectation of both the patient and the treating mental health professional in those communications. The second involves the application of the best interests of the child(ren) standard. Virtually every jurisdiction in the United States makes a child custody determination based upon the "best interest of the child".

It is interesting to note that in the previous cases it was a balance between the competing rights of two people, whereas in this case it was more about the right of one person vis-a-vis the best interest of a child, which incidentally has almost always been the deciding factor in Indian cases involving child custody.

Financial Privacy

Financial privacy involves the protection of consumers from unlawful access to financial accounts by private and public bodies, and the unlawful disclosure, sharing, or commercial use of financial information. Just as in the case of medical privacy, Indian law does cast a duty on bankers to protect the privacy of their customers. This duty of confidentiality is an extra layer of protection when it comes to financial information of individuals in addition to their right to privacy. Both these principles were used by the banks in one of the most important cases in the field of financial privacy, *i.e. District Registrar and Collector, Hyderabad* v. *Canara Bank and others*,[23] where a provision of law which allowed the person inspecting the documents to also seize and impound the documents was challenged by the banks. The provision also extended this power of inspection to include not only public officers but also to citizens and banks. It was challenged *inter alia*, on the ground that it intruded into the privacy and property of individuals. Considering the issue of allowing such inspections at banks which held the private documents of their customers or copies of such private documents, the question before the Court was whether disclosure of the contents of the documents by the banks would amount to a breach of confidentiality and would, therefore, be violative of privacy rights of their customers? Discussing this issue the Court held as follows:

> "It cannot be denied that there is an element of confidentiality between a Bank and its customers in relation to the latter's banking transactions……
>
> …Once we have accepted in *Govind* and in latter cases that the right to privacy deals with 'persons and not places', the documents or copies of documents of the customer which are in Bank, must continue to remain confidential vis-a`-vis the person, even if they are no longer at the customer's house and have been voluntarily sent to a Bank. If that be the correct view of the law, we cannot accept the line of *Miller* in which the Court proceeded on the basis that the right to privacy is referable to the right of 'property' theory. Once that is so, then unless there is some probable or reasonable cause or reasonable basis or material before the Collector for reaching an opinion

[23] http://www.judis.nic.in/supremecourt/imgs1.aspx?filename=26571

that the documents in the possession of the Bank tend, to secure any duty or to prove or to lead to the discovery of any fraud or omission in relation to any duty, the search or taking notes or extracts therefore, cannot be valid. The above safeguards must necessarily be read into the provision relating to search and inspection and seizure so as to save it from any unconstitutionality."

Secondly, the provision was also struck down because it enabled the Collector to authorize 'any person' whatsoever to inspect, to take notes or extracts from the papers in the public office since this was considered by the Court to be excessive delegation as there were no guidelines regulating this and the it allowed the facts relating to the customer's privacy to reach non-governmental persons and would, on that basis, be an unreasonable encroachment into the customer's rights. Therefore, the Court held this provision to be unconstitutional and struck it down.

Although banks are required to maintain confidentiality and thereby protect the privacy of their customers in their ordinary course of business, however sometime the duty to protect the right to privacy of their customers can come in direct conflict with the discharge of their functions. This situation has arisen a number of times when banks have sought to publish the photographs and information of wilful defaulters in newspapers, this practice has sometimes been objected to by the defaulters whose information is sought to be published on the ground that such publication would violate their right to privacy. There is currently a difference of opinion between various courts of law (i.e. High Courts in different States (provinces) have given different and opposing opinions on this issue). Some Courts have held that Banks are allowed to publish photographs of the defaulters even though it may violate the right to privacy of the defaulters since it would serve the interest of the bank and the economy as a whole by ensuring better recovery of bad loans.[24] On the other hand it has also been held by other Courts that (government owned) banks have the power to realize their dues only in a manner authorized by law and there is no provision in law which allows the bank to publish the photographs of defaulters in newspapers. It further held that such an action by the banks would violate the right to privacy of the individuals.[25]

Apart from the general duty of bankers to maintain confidentiality, there are certain legislations which also touch upon the need to maintain secrecy in financial transactions. The Credit Information Companies (Regulation) Act, 2005 and the Regulations thereunder which provide that specific instances under which credit information of individuals may be released by the credit information companies. Further, as far as financial institutions owned by the government are concerned the Public Financial Institutions (Obligation as to Fidelity and Secrecy) Act, 1983[26] as well as the State Bank of India Act, 1955[27] provide that these institutions are prohibited from divulging any information relating to the affairs of its clients except in accordance with laws of practice and usage. To enforce this all their employees must take an oath of secrecy before carrying out their duties.

Other than in the sectors discussed above, there exists some jurisprudence and legislation in relation to privacy in the fields of telecommunications, transparency as well as law enforcement which we shall discuss below under separate headings.

---

[24] *K.J. Doraisamy* v. *Asst. General Manager,* http://judis.nic.in/judis_chennai/qrydisp.aspx?filename=8673.

[25] *Venu P.R.* v. *Assistant General Manager, SBI and another*, 2013 (132) AIC 612 (Ker.H.C.).

[26] Sections 3 and 4, Public Financial Institutions (Obligation as to Fidelity and Secrecy) Act, 1983.

[27] Section 45, State Bank of India Act, 1955.

Legal Landscape for Surveillance

In India surveillance by the law enforcement authorities has always been an accepted practice, in fact, it was in the context of police surveillance that the two most landmark decisions on the right to privacy were pronounced by the Supreme Court. Even in those two cases, one upheld the surveillance activities of the police and the other struck them down mainly on a technical ground that they were being carried on without the proper authorisations. In the modern age however, most surveillance activities are carried on through tapping or interception of telecommunication messages and therefore the two most important legislations in the context of surveillance today are the Indian Telegraph Act, 1885 and the Information Technology Act, 2000.

Since the Indian Telegraph Act, 1885 is an older statute and some of the legal jurisprudence on surveillance originated around it, we shall first discuss the provisions of this statute that deal with surveillance before moving on to the provisions of the Information Technology Act, 2000.

The Indian Telegraph Act, 1885

The provision of the Indian Telegraph Act, 1885, ("**Telegraph Act**") which is relevant for the purpose of surveillance is Section 5 which empowers the Central Government and State Governments of India to order the interception of messages in two circumstances: (1) in the occurrence of any "public emergency" or in the interest of "public safety", and (2) if it is considered necessary or expedient to do so, in addition to the following instances:

- the interests of the sovereignty and integrity of India;
- the security of the State ;
- friendly relations with foreign states;
- public order;
- for preventing incitement to the commission of an offense;

It is important that the paragraph reads that these are two overarching pre-conditions for any interception to take place and must be met in addition to the listed instances.

The Supreme Court of India has specified the terms 'public emergency' and 'public safety', in the following terms:

> "Public emergency would mean the prevailing of a sudden condition or state of affairs affecting the people at large calling for immediate action. The expression 'public safety' means the state or condition of freedom from danger or risk for the people at large. When either of these two conditions are not in existence, the Central Government or a State Government or the authorised officer cannot resort to telephone tapping even though there is satisfaction that it is necessary or expedient so to do in the interests of its sovereignty and integrity of India etc. In other words, even if the Central Government is satisfied that it is necessary or expedient so to do in the interest of the sovereignty and integrity of India or the security of the State or friendly relations with sovereign States or in public order or for preventing incitement to the commission of an offence, it cannot intercept the message, or resort to telephone tapping unless a public emergency has occurred or the interest of public safety or the existence of the interest of public safety requires. Neither the occurrence of public emergency nor the interest of public safety are secretive conditions or situations. Either of the situations would be apparent to a reasonable person."[28]

[28] *PUCL* v. *Union of India,* http://www.judis.nic.in/supremecourt/imgs1.aspx?filename=14584

In 2007, Rule 419A was added to the Indian Telegraph Rules, 1951 framed under the Indian Telegraph Act which provided that orders on the interception of communications should only be issued by the Secretary in the Ministry of Home Affairs. However, it provided that in unavoidable circumstances an order could also be issued by an officer, not below the rank of a Joint Secretary to the Government of India, who has been authorised by the Union Home Secretary or the State Home Secretary.[29]

According to Rule 419A, the interception of any message or class of messages shall be carried out with the prior approval of the Head or the second senior most officer of the authorised security agency at the Central Level and at the State Level with the approval of officers authorised in this behalf not below the rank of Inspector General of Police, in the below mentioned emergent cases;

- in remote areas, where obtaining of prior directions for interception of messages or class of messages is not feasible; or
- for operational reasons, where obtaining of prior directions for interception of message or class of messages is not feasible;

However, the concerned competent authority should be informed of such interceptions by the approving authority within three working days and such interceptions should be confirmed by the competent authority within a period of seven working days. If the confirmation from the competent authority is not received within the stipulated seven days, such interception should cease and the same message or class of messages should not be intercepted thereafter without the prior approval of the Union Home Secretary or the State Home Secretary.[30]

Rule 419A also tried to incorporate certain safeguards to curb the menace of unrestricted surveillance by the law enforcement authorities which include the following:

- Any order for interception issued by the competent authority should contain reasons for such direction and a copy of such an order should be forwarded to the Review Committee within a period of seven working days;[31]
- Directions for interception should be issued only when it is not possible to acquire the information by any other reasonable means;[32]
- The directed interception should include the interception of any message or class of messages that are sent to or from any person n or class of persons or relating to any particular subject whether such message or class of messages are received with one or more addresses, specified in the order being an address or addresses likely to be used for the transmission of communications from or to one particular person specified or described in the order or one particular set of premises specified or described in the order;[33]
- The interception directions should specify the name and designation of the officer or the authority to whom the intercepted message or class of messages is to be disclosed to;[34]
- The directions for interception would remain in force for sixty days, unless revoked earlier, and may be renewed but the same should not remain in force beyond a total period of one hundred and eighty days;[35]

---

29 Rule 419A(1), Indian Telegraph Rules, 1951.

30 Rule 419A(1), Indian Telegraph Rules, 1951.

31 Rule 419A(2), Indian Telegraph Rules, 1951.

32 Rule 419A(3), Indian Telegraph Rules, 1951.

33 Rule 419A(4), Indian Telegraph Rules, 1951.

34 Rule 419A(5), Indian Telegraph Rules, 1951.

35 Rule 419A(6), Indian Telegraph Rules, 1951.

- The directions for interception should be conveyed to the designated officers of the licensee(s) in writing by an officer not below the rank of Superintendent of Police or Additional Superintendent of Police or the officer of the equivalent rank;[36]
- The officer authorized to intercept any message or class of messages should maintain proper records mentioning therein, the intercepted message or class of messages, the particulars of persons whose message has been intercepted, the name and other particulars of the officer or the authority to whom the intercepted message or class of messages has been disclosed, etc.;[37]
- All the requisitioning security agencies should designate one or more nodal officers not below the rank of Superintendent of Police or the officer of the equivalent rank to authenticate and send the requisitions for interception to the designated officers of the concerned service providers to be delivered by an officer not below the rank of Sub-Inspector of Police;[38]
- Records pertaining to directions for interception and of intercepted messages should be destroyed by the competent authority and the authorized security and Law Enforcement Agencies every six months unless these are, or likely to be, required for functional requirements;[39]

According to Rule 419A, service providers which are required by law enforcement to intercept communications are required to comply with the following:

- Service providers should designate two senior executives of the company in every licensed service area/State/Union Territory as the nodal officers to receive and handle such requisitions for interception;[40]
- The designated nodal officers of the service providers should issue acknowledgment letters to the concerned security and Law Enforcement Agency within two hours on receipt of intimations for interception;[41]
- The system of designated nodal officers for communicating and receiving the requisitions for interceptions should also be followed in emergent cases/unavoidable cases where prior approval of the competent authority has not been obtained;[42]
- The designated nodal officers of the service providers should forward every fifteen days a list of interception authorizations received by them during the preceding fortnight to the nodal officers of the security and Law Enforcement Agencies for confirmation of the authenticity of such authorizations;[43]
- Service providers are required to put in place adequate and effective internal checks to ensure that unauthorized interception of messages does not take place, that extreme secrecy is maintained and that utmost care and precaution is taken with regards to the interception of messages;[44]
- Service providers are held responsible for the actions of their employees. In the case of an established violation of license conditions pertaining to the maintenance of secrecy and confidentiality of information and unauthorized interception of communication, action shall be taken against service providers as per the provisions of the Indian Telegraph Act, and this shall not only include a fine, but also suspension or revocation of their license;[45]

---

36 Rule 419A(7), Indian Telegraph Rules, 1951.

37 Rule 419A(8), Indian Telegraph Rules, 1951.

38 Rule 419A(9), Indian Telegraph Rules, 1951.

39 Rule 419A(18), Indian Telegraph Rules, 1951.

40 Rule 419A(10), Indian Telegraph Rules, 1951.

41 Rule 419A(11), Indian Telegraph Rules, 1951.

42 Rule 419A(12), Indian Telegraph Rules, 1951.

43 Rule 419A(13), Indian Telegraph Rules, 1951.

44 Rule 419A(14), Indian Telegraph Rules, 1951.

45 Rule 419A(15), Indian Telegraph Rules, 1951.

- Service providers should destroy records pertaining to directions for the interception of messages within two months of discontinuance of the interception of such messages and in doing so they should maintain extreme secrecy.[46]

Information Technology Act, 2000

The Information Technology Act, 2000 ("**IT Act**") widely regulates the interception, monitoring, decryption and collection of information of digital communications in India. More specifically, section 69 of the IT Act empowers the Central Government and the State Governments to issue directions for the monitoring, interception or decryption of any information transmitted, received or stored through a computer resource. Section 69 of the IT Act expands the grounds upon which interception can take place as compared to the Telegraph Act. As such, the interception of communications under Section 69 is carried out in the interest of:

- The sovereignty or integrity of India;
- Defense of India;
- Security of the State;
- Friendly relations with foreign States;
- Public order;
- Preventing incitement to the commission of any cognizable offense relating to the above; and
- For the investigation of any offense.

It must be noted that although the grounds for interception are roughly the same as the Telegraph Act (except for the condition of prevention of incitement of only *cognizable* offences, defense of India and the addition of investigation of any offence) the IT Act does not have the overarching condition that interception can only occur in the case of public emergency or in the interest of public safety. Additionally, section 69 of the IT Act mandates that any person or intermediary who fails to assist the specified agency with the interception, monitoring, decryption or provision of information stored in a computer resource shall be punished with an imprisonment for a term which may extend to seven years and shall be liable for a fine.

Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009

Just like with Rule 419A of the Indian Telegraph Rules, the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 ("**IT Interception Rules**") framed under Section 69 and 69B stipulate as to who may issue directions of interception and monitoring, how such directions are to be executed, the duration they remain in operation, to whom data may be disclosed, confidentiality obligations of intermediaries, periodic oversight of interception directions by a Review Committee under the Telegraph Act, the retention of records of interception by intermediaries and to the mandatory destruction of information in appropriate cases.

According to the IT Interception Rules, the secretary of the Ministry of Home Affairs has been designated as the "competent authority" to issue directions permitting the interception, monitoring, and decryption of communications. At the State and Union Territory level, the State Secretaries respectively in charge of the Home Departments are designated as

[46] Rule 419A(19), Indian Telegraph Rules, 1951.

"competent authorities" to issue interception directions.[47] In unavoidable circumstances the Joint Secretary to the Government of India, when so authorised by the Competent Authority, may issue an order. Interception may also be carried out with the prior approval of the Head or the second senior most officer of the authorised security agency at the Central Level and at the State Level with the approval of officers authorised in this behalf not below the rank of Inspector General of Police, in the below mentioned emergent cases;

- in remote areas, where obtaining of prior directions for interception of messages or class of messages is not feasible; or
- for operational reasons, where obtaining of prior directions for interception of message or class of messages is not feasible;

However, in the above circumstances the officer would have to inform the competent authority in writing within three working days about the emergency and of the interception, monitoring or decryption and obtain the approval of the competent authority within a period of seven working days. If the approval of the competent authority is not obtained within the said period of seven working days, such interception or monitoring or decryption shall cease and the information shall not be intercepted or monitored or decrypted thereafter without the prior approval of the competent authority.[48] If a state wishes to intercept information that is beyond its jurisdiction, it must request permission to issue the direction from the Secretary in the Ministry of Home Affairs.[49]

If authorised by the competent authority, any agency of the government may intercept, monitor, or decrypt information transmitted, received, or stored in any computer resource only for the purposes specified in section 69(1) of the IT Act.[50] The IT Interception Rules further provide that the competent authority may give any decryption direction to the decryption key holder.[51]

The officer issuing an order for interception is required to issue requests in writing to designated nodal officers of the service provider.[52] Upon receiving an order for interception, service providers are required to provide all facilities, co-operation, and assistance for interception, monitoring, and decryption. This includes assisting with: the installation of the authorised agency's equipment, the maintenance, testing, or use of such equipment, the removal of such equipment, and any action required for accessing stored information under the direction.[53] Additionally, decryption key holders are required to disclose the decryption key and provide assistance in decrypting information for authorized agencies.[54]

---

47 Secretary in the Ministry of Home Affairs in case of the Central Government, Secretary in charge of the Home Department in case of a State Gov or Union territory; Rule 2(d), Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

48 Rule 3 of the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

49 Rule 6, Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

50 Rule 4, Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

51 Rule 5, Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

52 Rule 13, Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

53 Rule 19, Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

54 Rule 17, Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

Any direction issued by the competent authority must contain the reasons for direction, and must be forwarded to the review committee seven days after being issued.[55] In the case of issuing or approving an interception order, in arriving at its decision the competent authority must consider all alternate means of acquiring the information.[56] The order must relate to information sent or likely to be sent from one or more particular computer resources to another (or many) computer resources.[57] The reasons for ordering interceptions must be recorded in writing, and must specify the name and designation of the officer to whom the information obtained is to be disclosed, and also specify the uses to which the information is to be put.[58] The directions for interception will remain in force for a period of 60 days, unless renewed. If the orders are renewed they cannot be in force for longer than 180 days. [59]

Authorized agencies are prohibited from using or disclosing contents of intercepted communications for any purpose other than investigation, but they are permitted to share the contents with other security agencies for the purpose of investigation or in judicial proceedings. Furthermore, security agencies at the union territory and state level will share any information obtained by following interception orders with any security agency at the centre.[60]

All records, including electronic records pertaining to interception are to be destroyed by the government agency "every six months, except in cases where such information is required or likely to be required for functional purposes".[61] In addition, all records pertaining to directions for interception and monitoring are to be destroyed by the service provider within a period of two months following discontinuance of interception or monitoring, unless they are required for any ongoing investigation or legal proceedings.[62] The contents of intercepted, monitored, or decrypted information will not be used or disclosed by any agency, competent authority, or nodal officer for any purpose other than its intended purpose.[63]

The agency authorised by the Secretary of Home Affairs is required to appoint a nodal officer (not below the rank of superintendent of police or equivalent) to authenticate and send directions to service providers or decryption key holders.[64] Every fifteen days the officers designated by the intermediaries are required to forward to the nodal officer in

---

55 Rule 7, Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

56 Rule 8, Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

57 Rule 9, Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

58 Rule 10, Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

59 Rule 11, Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

60 Rule 25(2)&(6), Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

61 Rule 23, Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

62 Rule 23(2), Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

63 Rule 25, Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

64 Rule 12, Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

charge a list of interceptions orders received by them. The list must include the details such as reference and date of orders of the competent authority.[65]

The service provider is required to put in place adequate internal checks to ensure that unauthorised interception does not take place, and to ensure the extreme secrecy of intercepted information is maintained.[66] The contents of intercepted communications are not allowed to be disclosed or used by any person other than the intended recipient.[67] Additionally, the service provider is required to put in place internal checks to ensure that unauthorized interception of information does not take place and extreme secrecy is maintained. This includes ensuring that the interception and related information are handled only by the designated officers of the service provider.[68]

Apart from the above two statues, a number of criminal statues provide for interception of communications and how such intercepted communications may be used. The Unlawful Activities Prevention Act, 1967 allows for information collected through interception of communications (under the IT Act or the Telegraph Act) to be produced as evidence for an offence under the Act.[69] 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. Apart from this Act there are a number of state legislations such as the Maharashtra Control of Organized Crimes Act, 1999, the Andhra Pradesh Control of Organised Crime Act, 2001, etc. Apart from the criminal statutes, there are certain other laws which address surveillance activities by Indian law enforcement agencies which are briefly described below.

Indian Post Office Act, 1898

Section 26 of the Indian Post Office Act, 1898, empowers the Central Government and the State Governments of India to intercept postal articles. In particular, section 26 of the Indian Post Office Act, 1898, states that on the occurrence of any public emergency or in the interest of public safety or tranquility, the Central Government, State Government or any officer specially authorised by the Central or State Government may direct the interception, detention or disposal of any postal article, class or description of postal articles in the course of transmission by post. Furthermore, section 26 states that if any doubt arises regarding the existence of public emergency, public safety or tranquility then a certificate to that effect by the Central Government or a State Government would be considered as conclusive proof of such condition being satisfied.

Code of Criminal Procedure, 1973

Section 91 of the Code of Criminal Procedure, 1973 regulates targeted surveillance. In particular, section 91 states that a Court in India or any officer in charge of a police station may summon a person to produce any document or any other thing that is necessary for the

---

65 Rule 18, Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

66 Rule 20& 21, Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

67 Rule 25, Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

68 Rule 20, Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

69 Section 46, Unlawful Activities Prevention Act, 1967.

purposes of any investigation, inquiry, trial or other proceeding under the Code of Criminal Procedure. Under section 91, law enforcement agencies in India can access stored data. The Code also allows District Magistrates and Courts to issue directions requiring document, parcel or "things" within the custody of any postal or telegraph authority to be produced before it if needed for the purpose of any investigation, inquiry, trial or other proceeding under the Code.[70] If the Commissioner of Police or Superintendent of Police believes that such a document, parcel or "thing" is required for the above mentioned purposes he may require the postal or telegraph authority to detain such item pending an order from a court.[71] There is little judicial clarity on the subject but it has been argued that it is possible to interpret the provisions in a way that even private ISPs can be considered as postal or telegraph authorities and thus become subject to interception under this section.[72] It must however be noted that the level of protection granted to postal or telegraph authorities under section 92 is higher than that provided to ordinary citizens under section 91 since even a police officer in charge of a police station can ask for production of items whereas under section 92 it has to be either the District Magistrate or a specified Court.

Indian Wireless Telegraphy Act, 1933

Under section 3 of the Indian Wireless Telegraphy Act, 1933, the possession of wireless telegraphy apparatus without a license is considered an offense. As such, the unauthorised establishment, maintenance or operation of wireless communications networks for the purpose of monitoring, intercepting and surveillance of communications is in violation of the Indian Wireless Telegraphy Act, 1933.

Central Motor Vehicle Act 1898 and 2012 Rules

In October 2012, Rule 138A of the Central Motor Vehicle Rules, 1989, concerning radio frequency identification tags, was proposed. This proposed Rule mandates the installation of radio frequency identification ("RFID") tags on all light and heavy motor vehicles to enable their instant identification and monitoring by electronic collection toll booths, the police and any other authority or person that is able to query and read RFID tags[73].

1.2. License Agreements for Internet Service Providers (ISPs) and Telecom Service Providers (TSPs)

The Department of Telecommunications of the Ministry of Communications and Information Technology of the Government of India has issued license agreements with which Internet Service Providers (ISPs) and Telecom Service Providers (TSPs) operating in India need to comply. Such license agreements mandate the terms and conditions under which ISPs and TSPs in India can operate and in certain circumstances, ISPs and TSPs are required to carry out mass surveillance in order to be in compliance with these license agreements[74].

ISP License Agreement

Internet Service Providers (ISPs) in India are required to comply with the License Agreement

---

[70] Section 92, Code of Criminal Procedure, 1973.

[71] Section 91, Code of Criminal Procedure, 1973.

[72] Prashant Iyengar, "IP Addresses and Expeditious Disclosure of Identity in India" http://cis-india.org/internet-governance/ip-addresses-and-identity-disclosures

[73] Bhairav Acharya, "*Comments on the Proposed Rule 138A of the Central Motor Vehicle Rules, 1989, Concerning Radio Frequency Identification Tags*", The Centre for Internet and Society, 03 December 2012, http://cis-india.org/internet-governance/blog/comments-on-motor-vehicle-rules

[74] Government of India, Ministry of Communications and Information Technology, Department of Telecommunications, *Licensing*, http://www.dot.gov.in/licensing

for Provision of Internet Services in order to operate, which is issued by the Department of Telecommunications of the Ministry of Communications and Information Technology[75]. This License Agreement is governed by the Indian Telegraph Act, 1885, the Indian Wireless Telegraphy Act, 1933, and by the Telecom Regulatory Authority of India Act, 1997, as modified throughout time.

Clause 2.2 (vii) of India's License Agreement for Provision of Internet Services states the following:

"The Licensee shall ensure that Bulk Encryption is not deployed by ISPs. Further, individuals/ organizations/ groups are permitted to use encryption up to 40 bit key length in the symmetric key algorithms or its equivalent in other algorithms without obtaining permission from the Licensor. However, if encryption equipments higher than this limit are to be deployed, individuals/ organisations/ groups shall obtain prior written permission of the Licensor and deposit the decryption key, split into two parts, with the Licensor." [76]

According to this section, bulk encryption is prohibited and individuals, groups and/or organisations are prohibited from using encryption that exceeds a 40 bit key length in symmetric key algorithms. Furthermore, this section requires users to disclose their decryption key to the ISP in instances when they gain written permission to exceed the 40 bit key length limit.

Part VI of the ISP License Agreement provides the Government the right to inspect and monitor the ISPs' systems and ISPs are required to make their facilities available for such inspection. In particular, clause 32 under Part VI of the ISP License Agreement includes provisions which mandate the confidentiality of information and such provisions are identical to those contained in the National Long Distance License Agreement. Clause 33.4 requires TSPs to trace "nuisance, obnoxious or malicious calls, messages or communications" transported through their equipment and networks and to provide such data to authorised officers of the Government of India, including the police, customs and officers of the Intelligence Departments[77].

Clause 33.6 requires all ISPs in India to prevent all "objectionable, obscene, unauthorised or any other content, messages or communications infringing copyright, intellectual property right and international & domestic cyber laws" from being carried out in their networks. Under this clause, ISPs in India are required to provide all the tracing facilities for this and to report to authorised officers of the Government of India or of State Governments.

According to clause 34.4, ISPs in India are required to install and use "suitable monitoring equipment", as prescribed to them by the Department of Telecommunications. Furthermore, clause 34.6 of the ISP License Agreement allows designated persons of the Government of India or State Governments to monitor the telecommunications traffic in every node or in any other technically feasible point in the network. Under this clause, TSPs are required to monitor simultaneous calls by Government security agencies and the hardware and software required for monitoring calls must be engineered, provided, installed and maintained by the TSPs at their own cost.

Furthermore, clause 34.8 of the ISP License Agreement requires all ISPs to maintain a log of all users connected and the service they are using (such as mail, telnet and http). Under this

[75]Government of India, Ministry of Communications and Information Technology, Department of Telecommunications, *License Agreement for Provision of Internet Services, 1998*, http://www.dot.gov.in/data-services/internet-services

[76]Ibid: clause 2.2 (vii)

[77]Ibid

clause, ISPs are also required to log every outward login or telnet through their computers and such logs must be provided in real time to the Telecom Authority. Additionally, the logged in user must be identified in every case. This is supplemented by clauses 34.12 and 34.13, which require ISPs to make available a list of all subscribers to their services on a password protected website for easy access by Government authorities. This is further mandated in clause 34.22, which requires ISPs to make available “details of the subscribers using the service” to the Government or its representatives “at any prescribed instance”. In order for this to be feasible, clause 34.16 requires ISPs to activate services only after verifying the subscribers and collecting supporting documentation[78].

Clause 34.23 mandates that all commercial records exchanged through communications networks of an ISP network must be retained for at least one year for security reasons and that such records might destroyed thereafter. Clause 34.28 (viii) prohibits ISPs from transferring certain information to any person or place outside of India, which includes accounting information relating to the subscriber and other user information. Furthermore, clauses 34.28 (ix) and (x) require TSPs to provide traceable identity of their subscribers to the Government and should also be able to provide the geographical location of any subscriber at any given time. This is supplemented by clause 34.28 (xix) which stipulates that the monitoring of voice and data should only be carried out upon authorisation by the Union Home Secretary or by the Home Secretaries of the States/Union Territories[79].

Clause 34.27 of India's ISP License Agreement stipulates the installation of monitoring facilities at the ISPs' premises. In particular, clause 34.27 (ai) mandates that every ISP in India must be equipped with a monitoring centre at its own cost. Other such monitoring systems must be set up by ISPs carrying out Internet Telephony traffic through their Internet gateways. The entire cost relating to the installation and maintenance of such monitoring centres is being borne by the ISPs in India, according to this clause. Clause 34.27 (v) requires each router or switch of the ISP to be connected by the LAN operating at the same speed as the router or switch, and that the monitoring equipment should be connected to this network. Clause 34.27 (vi) states that it is acceptable for ISPs to set up their own central monitoring centre, if they are able to monitor all the traffic in all the routers or switches from a central location. According to clause 34.27 (b), when the ISP node router/switch has an outbound capacity of less than 2 Mbps, the monitoring equipment will be provided by security agencies.

Clause 34.28 (xiii) of the Indian ISP License Agreement prohibits off-the-air interception, as it states that ISPs are not allowed to use remote access facilities for the monitoring of content. Clause 34.28 (xvi) states that TSPs should ensure that the necessary hardware and software is available in their equipment for carrying out lawful interception and monitoring from a centralised location. Furthermore, clause 34.28 (xx) requires ISPs and TSPs to provide access to their network, as well as access to books of their accounts, to security agencies in India[80].

Various amendments have been incorporated in India's License Agreement for the Provision of Internet Services. Such amendments relate to the guidelines issue by the Department of Telecommunications for the grant of License for operating Internet services, as well as with respect to license fees and security related concerns for the expansion of telecom services in various zones of India. Furthermore, the Department of Telecommunications mandates the use of Telecom Tower Standards issued by Telecommunications Engineering Centres, as well as the security clearance of TSPs prior to the placement of their purchase order for

[78]Ibid
[79]Ibid
[80]Ibid

procuring telecom equipment and software[81].

TSP License Agreements

Telecom Service Providers (TSPs) in India have to comply with two license agreements in order to operate: the Cellular Mobile Telephone Service (CMTS) License Agreement[82] and the License Agreement for the Provision of Basic Telephone Services (BTS)[83]. The first license agreement applies to cellular mobile communications, whereas the second applies to landlines.

Clause 22 of the CMTS License Agreement refers to the application of the Indian Telegraph Act, 1885. As such, clause 22.1 requires TSPs to prevent "objectionable or obscene" messages or communications from being carried out in their networks. In order to do this, TSPs are required, under this clause, to provide the tracing facilities which can monitor telecommunications. Clause 22.2 extends this by mandating that TSPs provide the "necessary facilities" to designated authorities of the central or state government(s) for the interception of messages passing through their networks[84].

India's License Agreement for the Provision of Telephone Services (BTS) covers the interception of communications through basic telephone services. Clause 1.10.1 of the BTS License Agreement prohibits the use of bulk encryption, unless the use of encryption equipment has been authorised by the Department of Telecommunications. Clause 1.10.5 requires TSPs to provide authorised agencies of the Government of India full access to the switching centres, transmission centres and routes. Clause 1.10.7 mandates that TPSs are responsible for ensuring the privacy of communications and that unauthorised interception does not take place[85].

The BTS License Agreement was amended in 2001 and clause 23.14 stipulates that designated persons of the central or state government(s) shall have the right to monitor the telecommunications traffic in every switch and at any other point of the network set up by TSPs. Furthermore, clause 23.14 requires TSPs to make arrangements for monitoring simultaneous calls by Government security agencies and states that all hardware and software required for the monitoring of calls shall be engineered, provided, installed and maintained by TSPs at their own cost. Additionally, TSPs are required to ensure suitable redundancy in the complete chain of monitoring equipment for trouble free operations of monitoring at least 210 simultaneous calls.

Through the interception of all such calls, TSPs are required to disclose the following records to Indian governmental authorities:

---

[81] Government of India, Ministry of Communications and Information Technology, Department of Telecommunications, *"Pertaining to ISP License granted subsequent to guidelines dated 24.08.07"*, http://www.dot.gov.in/data-services/pertaining-isp-licence-granted-subsequent-guidelines-dated-240807

[82] Government of India, Ministry of Communications and Information Technology, Department of Telecomunications, *License Agreement for Provision of Cellular Mobile Telephone Service, 1994*, http://www.usof.gov.in/usof-cms/tender/cmtsAGREEMENT.pdf

[83] Government of India, Ministry of Communications and Information Technology, Department of Telecommunications, *License Agreement for Provision of Basic Telephone Service, 1992*, http://www.usof.gov.in/usof-cms/tender/usotender18Jan07/BasicServiceLicence.pdf

[84] Government of India, Ministry of Communications and Information Technology, Department of Telecomunications, *License Agreement for Provision of Cellular Mobile Telephone Service, 1994*, http://www.usof.gov.in/usof-cms/tender/cmtsAGREEMENT.pdf

[85] Government of India, Ministry of Communications and Information Technology, Department of Telecommunications, *License Agreement for Provision of Basic Telephone Service, 1992*, http://www.usof.gov.in/usof-cms/tender/usotender18Jan07/BasicServiceLicence.pdf

- Called / calling party numbers
- Time, duration and date of interception
- Precise location of target subscribers
- Subscriber numbers if any call-forwarding feature has been invoked by the target subscriber
- Date records for even failed call attempts

Under this clause, TSPs are required to provide all call data records (CDRs) to Indian security agencies when requested to do so[86].

Unified Access Services (UAS) License Agreement

The Unified Access Services (UAS) License Agreement applies to both Internet Service Providers (ISPs) and Telecom Service Providers (TSPs) operating in India and serves as a sort of "umbrella" license agreement[87].

In particular, clause 42 of the UAS License Agreement mandates the application of Section 5 of the Indian Telegraph Act, 1885, under which the Indian Government is authorised to intercept communications on the occurrence of any "public emergency" or in the interest of "public safety", if it is "necessary or expedient" to do so in the interest of the following:

- sovereignty and integrity of India
- security of the State
- friendly relations with foreign nations
- public order
- preventing incitement to the commission of any cognizable offense relating to the above
- investigation of any offense[88]

According to clause 42 of the UAS License Agreement, ISPs and TSPs in India are required to adopt all means and to facilitate in every manner the application of Section 5(2) of the Indian Telegraph Act, 1885. Clause 42.2. of the UAS License Agreement specifies that ISPs and TSPs are required to provide the necessary facilities to the designated authorities of the Central/State Government for the interception of messages passing through their networks. In short, clause 42 of the UAS License Agreement requires ISPs and TSPs in India to intercept communications through their networks and to provide such data to designated authorities[89].

While clause 42 of the UAS License Agreement mandates the interception of communications by ISPs and TSPs, clause 41. 4 states that ISPs and TSPs are responsible for ensuring the protection of privacy of communications and that unauthorised interception is prevented. Furthermore, clause 41.7 of the UAS License Agreement states that ISPs and TSPs are required to purchase "suitable monitoring equipment" as and when required by the Department of Telecommunications. Clause 41.10 of the UAS License Agreement states that the designated person of the Central/State Government shall have the right to monitor the

---

[86]Ibid

[87]Government of India, Ministry of Communciations and Information Technology, Department of Telecommunications, *License Agreement for Provision of Unified Access Services After Migration from CMTS, 2003,* http://www.dot.gov.in/access-services/unified-access-services

[88]The Indian Telegraph Act, 1885, Section 5, paragraph 2, http://www.ijlt.in/pdffiles/Indian-Telegraph-Act-1885.pdf

[89]Government of India, Ministry of Communications and Information Technology, Department of Telecommunications, *License Agreement for Provision of Unified Access Services After Migration from CMTS, 2003,* http://www.dot.gov.in/access-services/unified-access-services

telecommunications traffic in every MSC/ Exchange or in any other technically feasible point in the network. Moreover, clause 41.10 emphasizes that the hardware and software required for monitoring calls shall be engineered, provided, installed and maintained by the TSPs at their own cost. However, the cost of user end hardware and leased line circuits from the MSC/Exchange to the monitoring centres shall be covered by the respective state Government. Additionally, this clause requires TSPs to "*ensure suitable redundancy in the complete chain of Monitoring equipment for trouble free operations of monitoring of at least 210 simultaneous calls for Seven security agencies*".[90]

According to clause 41.10, in addition to the monitored call, the following records should be made available to the designated authorities of the Central/State Government of India:

- Called / calling party mobile / PSTN numbers
- Time/ date and duration of interception
- Location of target subscribers: Cell ID and, from time to time, the Department of Telecommunications may require the precision of location and GPS
- Telephone numbers if any call-forwarding feature has been invoked by the target subscriber
- Data records for failed call attempts
- CDR (call data records) of roaming subscriber[91]

Clause 41.10 of the UAS License Agreement also mandates that the hardware and software required for monitoring calls will be engineered, provided, installed and maintained by the TSPs at their own cost. Moreover, this clause mandates that TSPs are required to monitor *at least 480 calls simultaneously*, with at least 30 simultaneous calls for each of the nine designated law enforcement agencies[92].

In June 2013, clause 41.10 of the UAS License Agreement was amended to include provisions for the Centralized Monitoring System (CMS). In particular, the amended clause includes the following:

"But, in case of Centralized Monitoring System (CMS), Licensee shall provide the connectivity up to the nearest point of presence of MPLS (Multi Protocol Label Switching) network of the CMS at its own cost in the form of dark fibre with redundancy. If dark fibre connectivity is not readily available, the connectivity may be extended in the form of 10 Mbps bandwidth upgradeable up to 45 Mbps or higher as conveyed by the Government, till such time the dark fibre connectivity is established. However, LICENSEE shall endeavour to establish connectivity by dark optical fibre at the earliest. From the point of presence of MPLS network of CMS onwards traffic will be handled by the Government at its own cost."

As of a few years ago, the Government of India has decided to set up a Centralized Monitoring System (CMS) for the lawful interception and monitoring of communications. In order to implement this, clause 41.10 of the UAS License Agreement has been amended to mandate the establishment of the Centralized Monitoring System (CMS). In particular, TSPs are required to integrate Interception Store and Forward (ISF) servers with their Lawful Interception Systems and to connect them with the Regional Monitoring Centres (RMC), which are connected to the Centralized Monitoring System (CMS). This amendment specifies that TSPs are required to provide connectivity up to the nearest point of presence of MPLS (Multi Protocol Label Switching) network of the CMS at their own cost, in the form of dark optical fibre. From the MPLS network of the CMS onwards, traffic will be handled by the Government at its own cost.

---

[90] Ibid
[91] Ibid
[92] Ibid

Clause 41.11 states that upon Government notification, TSPs may be required to deny mobile services in areas specified by designated authorities. Additionally, clause 41.11 requires TSPs to provide the facility to carry out surveillance of Mobile Terminal activity within a specified area. On the one hand, clause 41.12 prohibits ISPs and TSPs from employing bulk encryption in their networks, but on the other hand, requires them to ensure the privacy of communications and that unauthorised interception does not take place. Furthermore, clause 41.14 requires ISPs and TSPs in India to provide intelligence agencies access to a list of all their subscribers. Clause 41.15 adds to this by stating that a photo identification of subscribers shall be a prerequisite before ISPs and TSPs provide those services. Clause 41.16 also specifies that the Department of Telecommunications will have access to the database relating to the subscribers of the ISPs and TSPs[93].

The UAS License Agreement also entails provisions for data retention by ISPs and TSPs in clauses 41.17, 41.19 and 41.20. In particular, clause 41.17 requires ISPs and TSPs to retain all commercial records with regards to the communications exchanged exchanged on the network for one year. Clause 41.19 requires providers to retain all outgoing call records, as well as information relating to each calling line identification. Clause 41.20 requires service providers to retain data on the geographical location of any subscriber at any given point of time and to store a complete audit trail of the remote access activities pertaining to the network operated in India for six months[94].

Unified License (Access Services) Agreement

The Unified License (Access Services) Agreement of 2013 also applies to both ISPs and TSPs in India. Part VI ("Security Conditions") mandates that the interception of communications is carried out by ISPs and TSPs which comply with this License Agreement[95].

While most of the clauses are similar with the equivalent in the Unified Access Services (UAS) License Agreement[96], some clauses include different and more detailed provisions. In particular, section 41.6 requires ISPs and TSPs to audit their networks or to get their networks audited from a security point of view once a year from a network audit and certification agency[97]. The clause also states that ISPs and TSPs can engage the service of any agency for this purpose, as long as that agency is certified to carry out the audit as per ISO 15408 and ISO 270001 certification standards. Clause 41.7 further requires service providers to gain certification to run their networks by authorised and certified agencies or labs in India. Furthermore, service providers are required to maintain copies of test results and test certificates for a period of ten years from the date of procurement of equipment. Moreover, clause 41.8 states that the hardware and software used by service providers may be subject to inspection and testing by their licensor at any given time. As such, clause 41.9 details the types of documentation that need to be made available by service providers and

---

[93] Government of India, Ministry of Communications and Information Technology, Department of Telecommunications, *License Agreement for Provision of Unified Access Services After Migration from CMTS, 2003,* http://www.dot.gov.in/access-services/unified-access-services

[94] Ibid

[95] Government of India, Ministry of Communications and Information Technology, Department of Telecommunications, *License Agreement for Unified License (Access Services), 2013,* http://www.dot.gov.in/sites/default/files/DOC270613-013.pdf

[96] Government of India, Ministry of Communications and Information Technology, Department of Telecommunications, *License Agreement for Provision of Unified Access Services After Migration from CMTS, 2003,* http://www.dot.gov.in/access-services/unified-access-services

[97] Government of India, Ministry of Communications and Information Technology, Department of Telecommunications, *License Agreement for Unified License (Access Services), 2013,* http://www.dot.gov.in/sites/default/files/DOC270613-013.pdf

the retention of records on the various types of equipment[98].

According to these clauses of the Unified License (Access Services) Agreement, the Government of India has mandated that all telecom security solutions of TSPs are tested against national or international telecom security standards. In other words, TSPs in India are required to get their equipment tested from certified labs located anywhere in the world. As such, the Department of Telecommunications is currently in the process of establishing the Telecom Testing & Security Certification Centre (TTSC). This is a project run by the Centre for Communications Security Research & Monitoring (CCSRM), which is also developing the Central Monitoring System (CMS). As of 1st October 2013, the testing and certification of telecom equipment is being undertaken by a pilot lab (IISc) in Bangalore, India, since the TTSC has not been established yet. In the mean while, TSPs in India are encouraged to get their equipment tested at IISc in Bangalore. In July 2013, Wipro and Tech Mahindra expressed their interest in establishing accredited Telecom Security Testing Labs through their presentations. In addition to all of this, a Telecom Security Policy has been drafted and sent to the National Information Board (NIB), but it has not been approved yet.

Clause 41.10 of the Unified License (Access Services) Agreement requires service providers to create monitoring facilities and to report to both the Department of Telecommunications and to CERT-In. Clause 41.11 lists the various penalties for security breaches, while clause 41.12 lists the location details that service providers are required to retain and to disclose to security agencies. In particular, service providers are required to provide CRD records in the form of longitude and latitude, in addition to the coordinate of the cell sites, which is already one of the mandated fields of CDR[99].

Clause 41.13 requires service providers to use “suitable monitoring equipment”, while clause 41.16 requires them to ensure suitable redundancy in the complete chain of monitoring equipment for “trouble free operations” of monitoring of at least 480 simultaneous calls with at least 30 simultaneous calls for each of the designated security/law enforcement agencies. In addition, service providers are required to have the capacity for provisioning of at least 3000 calls for monitoring to nine designated security/law enforcement agencies. The rest of the clauses under Part VI (“Security Conditions”) of the Unified License (Access Services) Agreement are similar to the equivalent in the UAS License Agreement. However, clause 41.26 states that service providers must comply with certain conditions, such as that of clause 41.26(x), which requires service providers to provide the geographical location of any subscriber to security agencies at any given point of time. Clause 41.26(xiii) states licensee companies are prohibited from using remote access facilities for the monitoring of content. Clause 41.26(xiv) states that a “suitable technical device” should be provided to designated security agencies in which a mirror image of remote access information is available on line for monitoring purposes[100].

Furthermore, clause 41.26(xvi) requires service providers to ensure that the necessary hardware and software is available in their equipment for undertaking the lawful interception and monitoring of communications from a *centralised location*. Clause 41.26(xvii) requires service providers to familiarize and train TERM cells, security agencies and officials to use the relevant operations and features of their systems. According to clause 41.26(xx), licensee companies are required to provide access to their networks and other facilities, as well as to books with accounts to security agencies. Interestingly enough, clause 41.26(xix) mandates that the monitoring of communications shall be in accordance with the rules under

[98] Ibid

[99] Government of India, Ministry of Communications and Information Technology, Department of Telecommunications, *License Agreement for Unified License (Access Services), 2013*, http://www.dot.gov.in/sites/default/files/DOC270613-013.pdf

[100] Ibid

the Indian Telegraph Act, 1885, in order to protect the privacy of voice and data.

Similarly to the UAS License Agreement, clause 42 of the Unified License (Access Services) Agreement mandates the application of Section 5(2) of the Indian Telegraph Act, 1885[101].

Legal Landscape for Cyber Security

Section 69B of the IT Act empowers the Central Government to authorise the monitoring and collection of information and traffic data generated, transmitted, received or stored through any computer resource for the purpose of cyber security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country. According to this section, any intermediary who intentionally or knowingly fails to provide technical assistance to the authorised agency which is required to monitor and collection information and traffic data shall be punished with an imprisonment which may extend to three years and will also be liable to a fine. The term "cyber security" has been defined in section 2(nb) the IT Act as "protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction". Further clarity on the meaning and import of the term can be gleaned from the Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009 which are discussed below.

The main difference between Section 69B and Section 69 (the provision for interception) is that while the latter requires the interception, monitoring and decryption of information generated, transmitted, received or stored through a computer resource, Section 69B specifically provides a mechanism for all metadata through a computer resource for the purpose of combating threats to "cyber security". Directions under Section 69 can be issued by the Secretary to the Ministry of Home Affairs, whereas directions under Section 69B can be issued by the Secretary of the Department of Information Technology under the Union Ministry of Communications and Information Technology.

The Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009

The Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009 issued under section 69B of the Information Technology Act stipulate that directions for the monitoring and collection of traffic data or information can be issued by an order made by the competent authority for any or all of the following purposes related to cyber security:

- forecasting of imminent cyber incidents;
- monitoring network application with traffic data or information on computer resource;
- identification and determination of viruses or computer contaminant;
- tracking cyber security breaches or cyber security incidents;
- tracking computer resource breaching cyber security or spreading virus or computer contaminants;
- identifying or tracking any person who has breached, or is suspected of having breached or likely to breach cyber security;
- undertaking forensic of the concerned computer resource as a part of investigation or internal audit of information security practices in the computer resources;
- accessing stored information for enforcement of any provisions of the laws relating to cyber security for the time being in force;

[101] Ibid

- Any other matter relating to cyber security.[102]

According to these Rules, any direction issued by the competent authority should contain reasons for such direction and a copy of such direction should be forwarded to the Review Committee within a period of seven working days.[103] Furthermore, these Rules state that the Review Committee shall meet at least once in two months and record its finding on whether the issued directions are in accordance with the provisions of sub-section (3) of section 69B of the IT Act. If the Review Committee is of the opinion that the directions are not in accordance with the provisions referred to above, it may set aside the directions and issue an order for the destruction of the copies, including corresponding electronic record of the monitored or collected traffic data or information.[104]

Cyber Crimes and Terrorism

Hacking: The IT Act does not define the term 'hacking', however, section 43 of the IT Act provides that any person who without permission of the owner of a computer, computer system accesses or secures access to, downloads, copies or extracts any data from, introduces or causes to be introduced any computer contaminant or computer virus into, damages, disrupts, denies access to such computer system or charges services availed of by one person to another person shall be liable to pay damages by way of compensation to the extent of Rs. 1,00,00,000/-.

Cyber Terrorism: Whoever with the intent to threaten the unity, integrity, security, or sovereignty of India or strike terror in the people denies authorised personnel access to computers, attempts to penetrate or access a computer resource without authorisation, or introduces malware to any computer, is considered to be committing an act of cyber terrorism.[105]

Voyeurism: Section 66E of the IT Act provides that whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person under circumstances violating the privacy of that person, and without consent would be liable to be imprisoned for up to 3 years and also pay a fine of up to 2 lakh rupees. The section further clarifies that a "private area" means the naked or undergarment clad genitals, pubic area, buttocks or female breast", "publishes" means reproduction in the printed or electronic form and making available to the public, "under circumstances violating privacy" means circumstances in which a person can have a reasonable expectation that he or she could disrobe in privacy, without being concerned that an image of his private areas was being captured or, any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

Section 354C of the Indian Penal Code, 1860 provides a similar protection, but provides varying penalties for the first and second offense. When comparing the two, the penalties are different – as the IPC provides for two levels of penalty for offenders. 66E also includes the publishing and transmission of a picture of any persons, whereas the IPC includes watching or capturing the image of a woman engaged in a private act.

---

[102] Rule 3(2), Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009.

[103] Rule 3(3), Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009.

[104] Rule 7, Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009.

[105] Section 66F, Information Technology Act, 2000.

Breach of Confidentiality and Privacy: The IT Act prohibits the disclosure of information that is obtained without consent of the relevant individual and any such disclosure is punishable with imprisonment for up to two years and a fine of up to one lakh rupees.[106] It further provides that any intermediary or person causing disclosure of information with the intent of causing wrongful loss or wrongful gain, without the consent of the person concerned, or in breach of a lawful contract would be liable to imprisonment for up to 3 years and fine which may extend up to five lakh rupees.

Identity Theft: Whoever, fraudulently or dishonestly makes use of an electronic signature, password or any other unique identification feature of any other person, is liable to be punished with imprisonment of up to three years and fine which may extend to one lakh rupees.[107]

Cheating by Impersonation: Any person who by means of any communication device or computer resource cheats by personation, is liable to be punished with imprisonment of up to three years and fine which may extend to one lakh rupees.[108]

Offences Relating to Interception: Service providers that do not comply with interception requests from authorised agencies would be liable to imprisonment for up to seven years and an unlimited amount of fine.[109] Any intermediary or employee of the same who intentionally and without authorisation attempts to intercept, authorise, or assist any person to intercept information in transmission at any place within India shall be liable to be imprisoned for up to two years and a fine which may extend to one lakh rupees.

Data Protection

The clearest legal provision addressing the issue of data protection in India is section 43A of the IT Act and the Rules framed thereunder. The provision requires a body corporate[110] who 'receives, possesses, stores, deals, or handles' any 'sensitive personal data' to implement and maintain 'reasonable security practices', failing which, they are held liable to compensate those affected. This provision has tried to introduce a mandatory data protection regime in Indian law. The section obliges corporate bodies who 'possess, deal or handle' any 'sensitive personal data' to implement and maintain 'reasonable' security practices, failing which they would be liable to compensate those affected by any negligence attributable to this failure.

However, it must be noted that it is only the narrowly-defined 'body corporates'[111] engaged in 'commercial or professional activities' who are the targets of this section thus excluding government agencies and non-profit organizations, etc. from the ambit of this section. This section along with the Rules under it represents an attempt to recognize that all persons have a right to protect the privacy of their personal information. It is a decisive first step towards building a legal regime that protects the privacy of individuals whilst enabling the secure collection, use and storage of personal information by state and private entities.

---

106 Section 72, Information Technology Act, 2000.

107 Section 66C, Information Technology Act, 2000.

108 Section 66D, Information Technology Act, 2000.

109 Section 69A(3), Information Technology Act, 2000.

110 Body corporate means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities.

111 Section 43A defines "body corporate" as any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities.

The "reasonable security practices" which the section obliges body corporates to observe are restricted to such measures as may be specified either "in an agreement between the parties" or in any law in force or as prescribed by the Central Government. By defining both "sensitive personal data" (in the Rules) and "reasonable security practice" in terms that require executive elaboration, the section in effect pre-empts the courts from evolving an iterative, contextual definition of these terms.[112]

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

Rule 3 of these Rules designates the following types of information as 'sensitive personal information':

- password;
- financial information such as Bank account / credit card / debit card / other payment instrument details of the users;
- physiological and mental health condition;
- sexual orientation;
- medical records and history;
- Biometric information;

This however, does not apply to "any information that is freely available or accessible in public domain or accessible under the Right to Information Act, 2005".

Rule 4 of these Rules requires a body corporate (or its agent) who collects, receives, possess, stores, deals or handle information, to provide a privacy policy for handling of such personal information ensure that the same is available for view by the providers of such information. The privacy policy is to be published on the website of the body corporate (or its agent) and should provide for (i) its practices and policies; (ii) type of personal or sensitive personal data or information collected; (iii) purpose of collection and usage; (iv) disclosure of information; and (v) reasonable security practices.

Rule 6 of these Rules states that personal information and sensitive personal data should only be disclosed in connection with the verification of identity, prevention, detection, investigation, prosecution and punishment of an existing offence. Offences can only be created by a parent statute or another statute. It may be relevant to note that these Rules add further grounds on which sensitive personal information may be released such as verification of identity, punishment of offences, etc. which do not exist in section 69 of the IT Act, 2000. However, since these Rules have been issued under the IT Act therefore such an expansion of the grounds beyond what is allowed in the parent Act (IT Act) should be considered as illegal.

Rule 7 of these Rules states that sensitive personal data should only be transferred to a body corporate or a person in India, or located in any other country in the world, that ensures the same level of data protection that is adhered to by the body corporate as per these Rules. Moreover, such transfer of data should only be allowed if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and the provider of information[34].

Rule 8 provides that body corporates shall be considered to have complied with their obligation towards reasonable security practices "if they have implemented such security

---

112 Prashant Iyengar, "Privacy and the Information Technology Act — Do we have the Safeguards for Electronic Privacy?", available at http://cis-india.org/internet-governance/blog/privacy/safeguards-for-electronic-privacy#35

practices and standards and have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business. In the event of an information security breach, the body corporate or a person on its behalf shall be required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security programme and information security policies."

Transparency Landscape

Just like freedom of the press, the principle of transparency in public offices can often come in direct conflict with the principle of privacy. This is particularly true in cases where relatively private information regarding public officials is concerned, as there may be situations where an enquiry into their private lives may become necessary to ensure that they were properly and honestly carrying out their public duties. In India, the Right to Information Act, 2005 (**RTI Act**) works primarily to promote transparency, contain corruption, and hold the Government accountable to citizens.

An overview of the RTI Act, especially sections 6 to 8 seems to give the impression that the legislature has tried to balance and harmonize conflicting public and private rights and interests by building sufficient safeguards and exceptions to the general principles of disclosure under the Act.[113] This is why it is generally suggested that section 8, when applied, should be given a strict interpretation as it is a fetter on not only a statutory right granted under the RTI Act but also a pre-existing constitutional right.[114] Logical as this argument may seem and appropriate in some circumstances, it does present a problem when dealing with the privacy exception contained in section 8(1)(j). That is because the right to privacy envisaged in this section is also a pre-existing constitutional right which has been traced to the same provisions of the Constitution from which the constitutional right of freedom of information emanates.[115] Therefore there is an ambiguity regarding the treatment and priority given to the privacy exception vs. the disclosure mandate in the RTI Act, as it requires the balancing of not only two competing statutory rights but also two constitutional rights.[116]

The Act establishes the right of citizens to request information held by public authorities, however it specifically prohibits disclosure of information which relates to personal information the disclosure of which has no relationship to any public activity or interest or which would cause unwarranted invasion of the privacy of the individual unless the disclosure would be in the interest of the larger public good. Thus the exception in S. 8(1)(j) prohibits the disclosure of personal information for two reasons (i) its disclosure does not relate to any public activity or interest or (ii) it would be an unwarranted invasion into privacy. The above two conditions however get trumped if a larger public interest is satisfied by the disclosure of such information.

There have been a number of cases which have tried to interpret the above exception while trying to decide exactly what information regarding a public official would be "personal" the

---

113 *Public Information Officer* v. *Andhra Pradesh Information Commission*, 2009 (76) AIC 854 (AP).

114 *Bhagat Singh* v. *Chief Information Commissioner*, 2008 (64) AIC 284 (Del).

115 Articles 14, 19(1)(a) and 21 of the Constitution of India, 1950.

116 Vipul Kharbanda, "Whitepaper on RTI and Privacy", available at http://cis-india.org/internet-governance/blog/white-paper-on-rti-and-privacy-v-1.2.

disclosure of which would cause unwarranted invasion of the official's privacy. The landmark case in this regard is the case of *Girish Ramchandra Deshpande* v. *Central Information Commissioner,*[117] where information was sought regarding the service career, assets and liabilities, movable and immovable properties of a public servant. The Supreme Court held that such information is personal in nature and can be only disclosed if there is a public interest involved and in this particular case, it was held that no such public interest could be demonstrated. This case categorically held that details relating to the performance of an employee in service as well as copies of memos, censures, show cause notices, etc. served on the employee as well as the employee's financial information would all come under the term "personal information" and should not be revealed unless a larger public interest is involved.

Therefore the performance of an employee/officer in an organization has been held to primarily be a matter between the employee and the employer falling under the expression "personal information", the disclosure of which has no relationship to any public activity or public interest. To understand this better, below is a brief list of the type of information that has been considered by the Courts as personal information which is liable to be exempt from disclosure under section 8(1)(j):

(1) (a) Salary details, (b) show cause notice, memo and censure, (c) return of assets and liabilities, (d) details of investment and other related details, (e) details of gifts accepted, (f) complete enquiry proceedings, (g) details of income tax returns;[118]

(2) All memos issued, show cause notices and orders of censure/punishment etc. are personal information. Cannot be revealed unless a larger public interest justifies such disclosure;[119]

(3) Disciplinary information of an employee is personal information and is exempt under section 8(1)(j);[120]

(4) Medical records cannot be disclosed due to section 8(1)(j) as they come under "personal information", unless a larger public interest can be shown meriting such disclosure;[121]

(5) Copy of personnel records and service book (containing Annual Confidential Reports, etc.) of a public servant is personal information and cannot be disclosed due to section 8(1)(j);[122]

Information regarding sexual disorder, DNA test between an officer and his surrogate mother, name of his biological father and step father, name of his mother and surrogate step mother and such other aspects were denied by the Courts as such information was

---

117 http://www.judis.nic.in/supremecourt/imgs1.aspx?filename=39615

118 *Girish Ramchandra Deshpande* v. *Central Information Commissioner*, 2012 (119) AIC 105 (SC).

119 *Girish Ramchandra Deshpande* v. *Central Information Commissioner*, 2012 (119) AIC 105 (SC).

120 *R.K. Jain* v. *Union Public Service Commission*, Delhi High Court, LPA No. 618 of 2012, dated 12-11-2012.

121 *Secretary General, Supreme Court of India* v. *Subhash Chandra*, Delhi High Court – Full Bench, LPA No.501/2009, dated 12-01-2010.

122 *Srikant Pandaya* v. *State of M.P.*, AIR 2011 MP 14.

considered beyond the perception of decency and was an invasion into another man's privacy.[123]

Regulatory Landscape for Surveillance and Cyber Security

In India, Government Departments involved in ensuring and overseeing cyber security are often also involved in some aspect of surveillance – as surveillance is legally justified for cyber and national security purposes in India. The key Government departments apart from the security agencies that play a role in ensuring India's cyber security and overseeing and regulating surveillance in India are the Department of Telecommunications (DoT) and the Department of Electronics and Information Technology (DeitY).

Department of Electronics and Information Technology:[124]

Broad functions of the Department of Electronics and Information Technology that are relevant to cyber security and surveillance include:

- Policy matters relating to Information Technology, Electronics and Internet.
- Initiatives for development of Hardware / Software industry including knowledge based enterprises, measures for promoting IT exports and competitiveness of the industry.
- Matters relating to Cyber Laws, administration of the Information Technology Act. 2000 and other IT related laws.

Relevant bodies located within the Department of Electronics and Information Technology relevant for the purpose of surveillance and cyber security are the following:

Controller of Certifying Authorities (CCA): Is responsible for licensing and regulating the working of Certifying Authorities. The Certifying Authorities (CAs) issue digital signature certificates for electronic authentication of users. Section 18 of IT Act provides legal sanctity to the digital signatures based on asymmetric cryptosystems. The digital signatures are now accepted at par with handwritten signatures and the electronic documents that have been digitally signed are treated at par with paper documents. The CCA aims at promoting the growth of E-Commerce and E- Governance through the wide use of digital signatures. It certifies the public keys of CAs using its own private key, which enables users in the cyberspace to verify that a given certificate is issued by a licensed CA. For this purpose it operates, the Root Certifying Authority of India (RCAI). The CCA also maintains the Repository of Digital Certificates, which contains all the certificates issued to the CAs in the country.[125]

The Cyber Appellate Tribunal has been established under section 48(1) to adjudicate on cases filed under the Act. The Court has jurisdiction to adjudicate on issues in which the claim for damages or injury is within the sum of Rs. 5 crore.[126]

The Standardisation Testing and Quality Certification Directorate (STQC) plays a key role in ensuring the security of IT infrastructure and software in India. STQC is responsible for

---

123 *Paardarshita Public Welfare Foundation* v. *Union of India and others*, AIR 2011 Del 82. It must be mentioned that this case was not exactly under the procedure prescribed under the RTI Act but was a public interest litigation although the courts relied upon the provisions of the RTI Act.

124 http://deity.gov.in/

125 http://cca.gov.in/

126 http://catindia.gov.in/Jurisdiction.aspx

auditing and certifying public and private organizations involved in the area of Electronics and IT including information security, software, and hardware.[127] For example, STQC has tested and certified the biometric devices used in the UID scheme.[128] STQC Certification Services are accredited for:

- ISO 9001 - Quality Management System (QMS)
- ISO 27001 - Information Security Management System (ISMS)- (Accreditation under Process)
- ISO 20000 – IT Service Management (ITSM) – (Accreditation under Process)
- Product Safety Certification Scheme based on IEC standards – (Accreditation under Process)

Certification issued by STQC is recognized internationally and STQC is in recognition agreements with the BSI, UK; TUV, Germany; JQA, Japan; Kaitech, S.Korea; CEPREL, China; KEMA, Netherlands etc.[129]

The Indian Computer Emergency Response Team is the key body in India responsible for overseeing and responding to cyber incidents in India. Organizational functions include: collection, analysis, and dissemination of information on cyber incidents, forecast and alerts of cyber security incidents, emergency measures for handling cyber security incidents, coordination of cyber incident response activities, and the issuing of relevant guidelines, advisories etc.[130] Reactive measures that CERT-IN undertakes include sharing information with other CERTS, artifact analysis, and incident tracing. Proactive measures that CERT IN undertake include security product evaluation, collaboration with vendors, profiling attackers, interaction with vendors and others at large to investigate and provide solutions for incidents.[131]

Department of Telecommunications

The Department of Telecommunications is the overseeing body for telecommunication and internet service providers in India. The Department of Telecommunications is responsible for the following areas that are relevant to cyber security:[132]

- Development of policy, licensing, and coordination of communication services;
- Framing of rules related to the security of telecom networks in India and coordination with Security Agencies on the same;
- Cooperation and coordination with international bodies related to telecommunications;
- Promotion of standardization, manufacturing, research and development in Telecommunications;
- Implementation of relevant laws including the Indian Telegraph Act, 1885, the Indian Wireless Telegraphy Act, 1933, and the Telecom Regulatory Authority of India Act, 1997.

Key bodies under the Department of Telecommunications include Telecom Enforcement Resource Management Cells, the Centre for Development of Telematics, the Telecommunication Engineering Centre, the National Telecommunications Institute for Policy Research, Innovation and Training, and the Telecom Regulatory Authority of India, and TDAT.

---

127 http://www.stqc.gov.in/content/about-stqc

128 http://www.stqc.gov.in/content/bio-metric-devices-testing-and-certification

129 http://www.stqc.gov.in/content/our-accreditations-and-recognitions-2

130 http://www.cert-in.org.in/

131 http://www.cert-in.org.in/

132 http://www.dot.gov.in/sites/default/files/DOC300414%20%281%29_0_3.pdf

Telecom Enforcement Resource Management Cells (TERM Cells)[133] among other functions, they are responsible for inspecting the premises of Telecom and Internet Service Providers, analysis of call/subscription/traffic data of various licensees, and for the technical arrangement for the lawful interception/monitoring of communications passing through the licensees network.[134] They are also responsible for the monitoring of ISPs and TSPs to ensure that licensees are in compliance with the license conditions and on matters related to national security, grievance redresses of subscribers, customer document verification to ensure that service providers are verifying their customers as legally mandated, and they serve as the technical interface between security agencies and telecom service providers. For example, in March 2014 TERM cells issued a notice on vulnerabilities that have been found in ADSL modems.[135]

Centre for Development of Telematics (CDOT) is an autonomous body under the Department of Telecommunications responsible for the development, manufacturing, and distribution of indigenous telecom technology. CDOT is responsible for architecting the Central Monitoring System and a number of other security and surveillance solutions.[136]

Telecommunication Engineering Centre is responsible for driving Telecom Standards, providing manufacturing support, and developing network building skill sets that are in the interest of India and the market. It is a Centre of Excellence and sets standards for telecom equipment along with certifying the same.[137]

National Telecommunications Institute for Policy Research, Innovation & Training - Ongoing projects of the NTIPRIT include a study into the challenges and recommendations in the implementation of the National Cyber Security Policy 2013, and the creation of a Sectoral Cyber Emergency Response Team in the Department of Telecommunications.[138] NTIPRIT also provides trainings to officials in the Department of Telecommunications and other officers in the government. These include trainings on Cyber Security[139], Wireless Security[140], and Lawful Interception[141]. NTIPRIT also offers training support to intelligence agencies and law enforcement agencies on advancements in telecom and ICT.[142]

The Telecom Regulatory Authority of India has the following responsibilities related to cyber security and surveillance:

- Ensuring compliance of terms and conditions of license terms and revocation of license for non-compliance of terms and conditions of license;
- Recommending the type of equipment to be used by the service providers after inspection of equipment used in the network;
- Recommending measures for the development of telecommunication technology and any other matter relatable to telecommunication industry in general.

133 http://www.dot.gov.in/term/term-security
134 http://www.dot.gov.in/term/term-security
135 http://www.dot.gov.in/sites/default/files/DOC200314_4.pdf
136 http://www.cdot.in/home.htm
137 http://www.tec.gov.in/
138 http://www.ntiprit.gov.in/
139 http://www.ntiprit.gov.in/eng/programs.php#INS
140 http://www.ntiprit.gov.in/eng/course_details.php?c_code=013&c_id=185
141 http://www.ntiprit.gov.in/eng/course_details.php?c_code=036&c_id=250
142 http://www.ntiprit.gov.in/

Security and law enforcement landscape

In India surveillance is carried out by central intelligence agencies and the state police. There are at least sixteen different intelligence agencies that have been established by executive order. Typically they are established under different and relevant government departments, they are centralized in structure and opaque in nature as they are not subject to the RTI Act or to audits by the CAG. Each State has a dedicated police force made up of different divisions and officers. While the interception activities of these agencies are (supposed to be) carried in accordance with the procedures contained in the Telegraph Act, 1885 and the Information Technology Act, 2000 and the Rules framed under those legislations, non interception as well as passive interception surveillance by the intelligence agencies are not governed by these legislations but usually by their own internal guidelines and operation manuals, etc.

It is difficult to make a complete list of all the intelligence agencies in India and the legislations that govern them since by their very nature intelligence agencies try to avoid legislative oversight. That said, the major intelligence agencies in India, as gleaned from information available in the public domain, including news reports, etc., are the following:

•*The National Investigation Agency*[143]: Located under the Ministry of Home Affairs, the NIA is responsible for investigating in counter terrorism and other national security issues at the national level. The agency is Governed by the National Investigation Agency Act, 2008.

• *National Technical Research Organization*[144]: Established in 2004 and located under the National Security Advisor of in the Prime Minister's Office, NTRO is a technical intelligence agency specializing in satellite and terrestrial monitoring, and developing technology for national security and intelligence (data management, cryptology, etc.). NTRO also serves as an advisor to the Prime Minister on security issues and provides technical intelligence to other Indian agencies.

• *Research and Analysis Wing*: Located under the Prime Ministers Office, RAW is India's external intelligence agency and is primarily responsible for foreign intelligence gathering and counter terrorism measures.

• *Intelligence Bureau:* Located under the Ministry of Home Affairs,[145] the IB is India's internal intelligence agency responsible for gathering internal intelligence and carrying out counter intelligence and terrorism mandates.

• *Central Bureau of Investigation*: The Central Bureau of Investigation (CBI), functioning under Dept. of Personnel, Ministry of Personnel, Pension & Public Grievances, Government of India, is the premier investigating police agency in India. It is an elite force playing a major role in preservation of values in public life and in ensuring the health of the national economy. It is also the nodal police agency in India which coordinates investigation on behalf of Interpol Member countries. The following broad categories of criminal cases are handled by the CBI:

(i) Cases of corruption and fraud committed by public servants of all Central Govt. Departments, Central Public Sector Undertakings and Central Financial Institutions.

(ii) Economic crimes, including bank frauds, financial frauds, Import Export & Foreign Exchange violations, large-scale smuggling of narcotics, antiques, cultural property and smuggling of other contraband items etc.

143 http://www.nia.gov.in/

144 http://searchsecurity.techtarget.in/definition/National-Technical-Research-Organisation-NTRO

145 http://mha.nic.in/attached

(iii) Special Crimes, such as cases of terrorism, bomb blasts, sensational homicides, kidnapping for ransom and crimes committed by the mafia/the underworld. [146]

• *Directorate of Revenue Intelligence*: The Directorate of Revenue Intelligence was constituted on 4th December 1957, for dealing exclusively with the work relating to the collection and study of information on smuggling activities and the deployment of all anti-smuggling resources at the all India level, besides arranging training for the intelligence and Investigation officers of the Custom Houses and Central Excise Collectorates deployed on similar work.[147]

•*Defence Intelligence Agency:* Nodal agency for all defence related intelligence and controls the Directorate of Signals Intelligence which is responsible for acquiring and decrypting enemy communications and the Defence Image Processing and Analysis Centre (DIPAC) which controls India's satellite-based image acquisition capabilities.[148]

• *Military Intelligence Directorate*: The agency was set up in 1941 to generate field intelligence for the Indian army. Post independence, it became a small army department primarily that investigated corruption within the force. The agency gathered momentum in the 1990s especially after the Kargil conflict with Pakistan. MI was initially tasked with generating only tactical or field intelligence in all countries bordering India. Its geographical mandate was set to 50 km from the border. These limits were quickly crossed in the mid-1990s when the organisation began playing an increasing role in countries within the subcontinent and its outer periphery.[149]

•*Directorate of Air Intelligence*: is the intelligence arm of the Indian Air Force. Its responsibilities include imagery intelligence collection MiG-25R and Jaguar reconnaissance aircraft.[150]

•*Directorate of Navy Intelligence:* Is the intelligence arm of the Indian Navy.[151]

• *Joint Cipher Bureau:* Responsible for signals intelligence and cryptanalysis and encryption of sensitive data.[152]

• *Aviation Research Centre*: Located under RAW – responsible for aerial surveillance, monitoring of borders, imagery intelligence.[153]

• *Enforcement Directorate*: A Multi Disciplinary Organization mandated with the task of enforcing the provisions of two special fiscal laws – Foreign Exchange Management Act, 1999 (FEMA) and Prevention of Money Laundering Act, 2002 (PMLA). The main functions of the Directorate are as under:

(i) Investigate contraventions of the provisions of Foreign Exchange Management Act, 1999(FEMA) which came into force with effect from 1.6.2000. Contraventions of FEMA are dealt with by way of adjudication by designated authorities of ED and penalties up to three times the sum involved can be imposed.

(ii) Investigate offences of money laundering under the provisions of Prevention of Money Laundering Act, 2002(PMLA) which came into force with effect from 1.7.2005 and to take actions of attachment and confiscation of property if the same is determined to be proceeds of crime derived from a Scheduled Offence under PMLA, and to prosecute the persons involved in the offence of money laundering.

---

146 http://cbi.nic.in/aboutus/cbiroles.php

147 http://dri.nic.in/home/aboutus

148 http://en.wikipedia.org/wiki/Defence_Intelligence_Agency_(India)

149 http://indiatoday.intoday.in/story/bangladesh-indian-army-military-intelligence-directorate-sheikh-hasina/1/170880.html

150 http://en.wikipedia.org/wiki/Directorate_of_Air_Intelligence

151 http://en.wikipedia.org/wiki/List_of_Indian_intelligence_agencies

152 *Ibid.*

153 *Ibid.*

There are 156 offences under 28 statutes which are Scheduled Offences under PMLA.

(iii) Adjudicate Show Cause Notices issued under the repealed Foreign Exchange Regulation Act, 1973 (FERA) up to 31.5.2002 for the alleged contraventions of the Act which may result in imposition of penalties. Pursue prosecutions launched under FERA in the concerned courts.

(iv) Sponsor cases of preventive detention under Conservation of Foreign Exchange and Prevention of Smuggling Activities Act, 1974(COFEPOSA) in regard to contraventions of FEMA.

(v) Render cooperation to foreign countries in matters relating to money laundering and restitution of assets under the provisions of PMLA and to seek cooperation in such matters.[154]

• *Crime Branch – Criminal Investigation Department:* These agencies exist in pretty much most states of India and deal with investigation of criminal matters.

Most of the above intelligence agencies do not have a defined oversight mechanism other than the departments that they report to. For example: CBI and RAW report to the Prime Minister's Office, Directorate of Revenue Intelligence reports to the Finance Ministry, and the Military Intelligence agencies report to the Ministry of Defence.

In addition to the above agencies, state level law enforcement have maintained passive interception capabilities, the Army also has passive interception capabilities as well as Line of Control to pick up the communications of civilians.[155] There have also been reports of surveillance equipment missing, gone to political parties or corporate institutions.

The Ministry of Home Affairs

The Ministry of Home Affairs is responsible for internal security of the country. It carries out its functions through various divisions described below:

Border Management Division: This Division deals with matters relating to coordination and concerted action by administrative, diplomatic, security, intelligence, legal, regulatory and economic agencies of the country for the management of international borders, creation of infrastructure like roads/fencing and floodlighting of borders, border areas development programme pilot project on Multi-purpose National Identity Card and Coastal Security.

Internal Security Division-I: Division deals with matters relating to internal security and law&order, including anti-national and subversive activities of various groups/extremist organizations, policy and operational issues on terrorism, security clearances, monitoring of ISI activities and Home Secretary-level talks with Pakistan on terrorism and drug trafficking as a part of the composite dialogue process.

Internal Security Division-II: Division deals with all matters concerning the Arms Act 1959, Arms Rules 1962, Explosive Substances Act 1908 and other related matters; letters of request for mutual legal assistance in criminal matters; National Security Act, 1980 and representations thereunder; administration of Narcotics Control Bureau; providing central assistance to victims of terrorist, communal and naxal violence; matters relating to breach of privilege of MPs, etc.

Left Wing Extremism Division: This Division was created w.e.f. October 19, 2006 in the Ministry to effectively address the LWE problem from development and security angles. The Division monitors the LWE situation and counter-measures being taken by the affected

---

154 http://www.enforcementdirectorate.gov.in/functions.html?p1=1151131423810719454

155 http://www.thehindu.com/news/national/the-governments-listening-to-us/article2678501.ece

States. The Division reviews implementation of various development schemes of Ministries/Departments of Govt. of India in the LWE affected areas.

North East Division: The Division deals with the internal security and law & order situation in North-Eastern States, including matters relating to insurgency and talks with various extremist groups operating in that region.

Police Division-II: This Division deals with the policy, personnel, operational (including deployment) and financial matters relating to all the Central Armed Police Forces (CAPFs) including BSF Air Wing. It also deals with the matters relating to welfare of the serving and retired CAPF personnel and the deployments in UN Peace Keeping Missions.

Digital Evidence Landscape

In India the Information Technology Act, 2000 (**ITA**) was passed as a law addressing digital content and to grant legal recognition to transactions carried out by means of electronic communication. Section 4 of the IT Act provides that where any law provides that information or any other matter shall be in writing, then, such requirement shall be deemed to have been satisfied if such information or matter is made available in electronic form and is available for use for a subsequent reference. In order to ensure that electronic records are authentic the Act provides for authentication of electronic records by affixing a Digital Signature by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.[156] In 2008 section 3A was inserted into the IT Act which allows for other means of authenticating electronic records. The IT Act also made a number of amendments to the Indian Evidence Act which are specified in the Second Schedule to the IT Act so as to enable production of electronic records as evidence in courtroom proceedings. The most important of these amendments are discussed below:[157]
(i) In section 3 of the Indian Evidence Act, the term "evidence" now includes "electronic records";
(ii) Section 47A has been inserted which provides: "47A. *Opinion as to digital signature when relevant.*- When the court has to form an opinion as to the digital signature of any person, the opinion of the Certifying Authority which has issued the digital signature Certificate is a relevant fact";
(iii) Sections 65A and 65B have been added which provide as follows:

> "*65A. Special provisions as to evidence relating to electronic record.*-The contents of electronic records may be proved in accordance with the provisions of section 65B.
> *65B. Admissibility of electronic records.*-(1) Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copies in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible.
> (2) The conditions referred to in sub-section (1) in respect of a computer output shall be the following, namely:- (a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;

---

156 Section 3, Information Technology Act, 2000.

157 Other sections of the Indian Evidence Act, 1872 which were amended are sections 17, 22, 34, 35, 39 and 59.

(b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;

(c) throughout the material part of the said period, the computer was operating properly or, if not; then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents;

(d) the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.

(3) Where over any period, the function of storing or processing information for the purposes of any activities regularly carried on over that the period as mentioned in clause (a) of sub-section (2) was regularly performed by computers, whether- (a) by a combination of computers operating over that period; or

(b) by different computer operating in succession over that period; or

(c) by different combinations of computers operating in succession over that period; or

(d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers, all the computers used for that purpose during that period shall be treated for the purposes of this section as constituting single computer, and references in this section to a computer shall be construed accordingly.

(4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say-

(a) identifying the electronic record containing the statement and describing the manner in which it was produced;

(b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;

(c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate, and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter sufficient for a matter to be stated to the best of knowledge and belief of the person stating it.

(5) For the purposes of this section,-

(a) information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without intervention) by means of any appropriate equipment;

(b) whether in the course of activities carried on by any official, information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, in duly supplied to that computer shall be taken to be supplied to it those activities;

(c) a computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

Explanation.-For the purposes of this section any reference to information being derived from other information shall be a reference to its being derived there from by calculation, comparison or any other process;"

(iv) Section 67A has been inserted which provides "*67A. Proof as to digital signature.*- Except in the case of a secure digital signature, if the digital signature of any subscriber is alleged to have been affixed to an electronic record the fact that such digital signature is the digital signature of the subscriber must be proved."

(v) Section 73A has been inserted which provides as follows:

"*73A. Proof as to verification of digital signature.*-In order to ascertain whether a digital signature is that of the person by whom it purports to have been affixed, the Court may direct-

(a) that person or the Controller or the Certifying Authority to produce the Digital Signature Certificate;

(b) Any other person to apply the public key listed in the Digital Signature Certificate and verify the digital signature purported to have been affixed by that person."

Explanation .-For the purposes of this section, "Controller" means the Controller appointed under sub-section (1) of section 17 of the Information Technology Act, 2000."

(vi) Section 81A has been inserted which provides as follows:

"*81A. Presumption as to Gazettes in electronic forms.*-The Court shall presume the genuineness of every electronic record purporting to be the Official Gazette, or purporting to be electronic record directed by any law to be kept by person, if such electronic record is kept substantially in the form required by law and is produced from proper custody."

(vii) Section 85A has been inserted which provides as follows:

"*85A. Presumption as to electronic agreements.*- The court shall presume that every electronic record purporting to be an agreement containing the digital signatures of the parties was so concluded by affixing the digital signature of the parties.

"*85B. Presumption as to electronic records and digital signatures.*-(1) IN any proceedings involving a secure digital signature, the Court shall presume unless the contrary is proved that-

(a) the secure digital signature is affixed by subscriber with the intention of signing or approving the electronic record;

(b) Except in the case of a secure electronic record or a secure digital signature, nothing in this section shall create any presumption relating to authenticity and integrity of the electronic record or any digital signature.

85C. Presumption as to Digital Signature Certificates.-The Court shall presume, unless contrary is proved, that the information listed in a Digital Signature Certificate is correct, except for information specified as subscriber information which has not been verified, if the certificate was accepted by the subscriber."

(viii) Section 88A has been inserted which provides as follows:

"*88A. Presumption as to electronic messages.* - The Court may presume that b electronic message forwarded by the originator through an electronic mail server to the addresses to whom the message purports to be addressed corresponds with the message as fed into his computer for transmission; but the Court shall not make any presumption as to the person by whom such message was sent.

Explanation.-for the purposes of this section, the expression "addressee' and "originator" shall have the same meanings respectively assigned to them in clauses (b) and (za) of sub-section (1) of section 2 of the information Technology Act, 2000."

(ix) Section 90A has been inserted which provides as follows:

"*90A. Presumption as to electronic records five years old.*- Where any electronic record, purporting or proved to be five years old, is produced from any custody which the court in the particular case considers proper, the Court may presume that the digital signature which purports to be the digital signature of any particular person was so affixed by him or any person authorised by him this behalf.

Explanation.-Electronic records are said to be in proper custody if they are in the place in which, and under the care of the person with whom, they naturally be; but no custody is improper if it is proved to have had a legitimate origin, or the circumstances of the particular case are such as to render such and origin probable."

(x) Section 131 has been substituted with the new section 131 as provided below:

"*131. Production of documents or electronic records which another person, having possession, could refuse to produce.*- No one shall be compelled to produce documents in his possession or electronic records under his control, which any other person would be entitled to refuse to produce if they were in his possessions or control, unless such last-mentioned person consents to their production."

These changes in the Indian Evidence Act have been made to provide a legal regime for the production of electronic records in legal proceedings in India which provides for acceptance of electronic records as evidence, acceptance of digital signatures, digital messages and agreements, etc.

Even before these provisions were introduced in the Indian Evidence Act, the Supreme Court in India had to decide upon the issue of whether evidence collected through an illegal wire tap could be introduced and accepted by a Court. In the case of *R.M. Malkani* v. *State of Maharashtra*,[158] 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 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. The Court dealt with this argument but held that there is no bar in admitting relevant contemporaneous evidence even if it is obtained illegally, even though it is up to the Court to decide how much reliance is to be placed on such evidence.

158 http://www.judis.nic.in/supremecourt/imgs1.aspx?filename=6708