DRAFT

Telecommunications and Internet Privacy in India

Introduction

Today in India, privacy is threatened perhaps the most by the internet and telecommunications. On one hand the increased use of these technologies allows individuals to become more visible, accessible, and interconnected. On the other hand, the same technologies allow governments, corporations, and other entities unrestricted access into the lives of the public. For example, individuals are plagued with spam messages and unsolicited marketing calls/text messages, risk fraud and phishing attacks as they transact online, have personal information gathered, used, and sold without permission or knowledge, and risk having service providers retain user data and history.

Furthermore, online privacy is threatened as the users often do not have control over the information that they generate and the line between what is private information, and what is public information is often fuzzy. This has created a situation where information displayed on social networking sites can be used as evidence against an individual or to make decisions about the individual. Employers now look into an individual's Facebook profile as part of the process for deciding whether to hire or promote a person and law enforcement agencies make decisions based off of social media content. For example, in 2012 a number of individuals were arrested in India for comments tweeted or posted on Facebook. This included two girls, one of whom had posted a comment on the death of politician Bal Thackeray, and her friend who liked the comment.[i] Among other questions, these incidents raise the question of whether speech on social media is private or public.

Another large component of privacy on the internet is with regards to how law enforcement can access online communications and habits through interception, access, or monitoring. The legitimacy for interception in India hinges on its conformance with constitutional provisions that allow reasonable restrictions on the exercise of fundamental rights to India's citizens. The interception of private or personal communications involves restrictions on the right to freedom of expression and the right to privacy. While the Constitution does not explicitly guarantee a right to privacy, the courts in India have consistently read that right into the definition of the fundamental right to life and personal liberty.[ii] These rights are not absolute and the courts have held that parliament may impose reasonable restrictions on the exercise of fundamental rights.

Countries around the world have taken steps to address privacy issues that arise from the internet, including adopting legislation implementing do not track standards, the right to be forgotten, breach notification, standards around lawful access, and data retention policies. This chapter will explore what legislation and protections India has in place to protect the privacy of individuals' communications and online behavior, what case law has added to the understanding of communication and internet privacy, how these policies and legislation are being implemented, and what the international best practices are.

Legislation

The Information Technology Act, 2000

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. The ITA contains a number of provisions that can, in some cases, safeguard online and computer related privacy, or in other cases, can dilute online and computer privacy. For example, the ITA contains interception provisions for authorized agencies, allows the government to set the national encryption standard, regulates what content can and cannot be put online, and prohibits the anonymous use of the internet. On the other hand, the ITA creates penalty for child pornography, hacking, and fraud, and lays out data protection standards for corporates conducting digital or online business.[1] The Information Technology Act applies to any offence or contravention of the Act committed in or outside of India if the offence involves a computer, computer system, or computer network located in India[iii]. Below is a description and analysis of provisions that relate to privacy.

Digital Signatures: The ITA provides for the use of digital signatures for authenticating electronic records. This is done through the use of asymmetric encryption, so that the electronic record can be verified using the public key of the subscriber.[2] In India, the issuance of Digital Signatures is the responsibility of the Controller of Certifying Authorities[3], who can either issue digital signatures to End Users directly, or through the Registration Authorities/Local Registration Authority. A few Certification Agencies in India include: National Informatics Centre, Institute for Development & Research in Banking Technology, TCS, MtnlTrustline, GNFC, SafeScrypt, e – MudhraCA.[4]

Hacking: The ITA does not define the term 'hacking' activities such as accessing a computer, downloading copies or extracts of data, introducing a computer virus in the system, etc. are made punishable under the ITA.[5]

Voyeurism: The ITA 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.[iv]

Section 354C of the IPC 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

---

[1] Note: The analysis of these data protection standards can be found in the Consumer Privacy chapter

[2] ITA section 3

[3] http://cca.gov.in/cca/index.php

[4] http://cca.gov.in/cca/index.php?q=faq-page#n41

[5] ITA section 66.

image of a woman engaged in a private act.[v] When reading the two provisions together, it is not clear if an individual can be punished for the first time under ITA 2008 and for the second time under IPC.[vi]

Interestingly, there have been many sex and MMS scandals in India which have not been heard under section 66E, presumably because the section only came into being in the year 2008. According to a note issued by the Ministry of Home Affairs in 2012, section 66E can also be used for cases of cyber bullying and cyber stalking.[vii]

Child Pornography: The ITA prohibits the publishing and transmission of digital material that depicts children in a sexually explicit way. This includes: publishing, transmitting, creating text or images, collecting, seeking, browsing, downloading, advertising, promoting, exchanging, or depicting the same. Furthermore, cultivating, enticing, or inducing children into a sexually explicit act online is prohibited. The term 'children' is defined as any person under the age of 18.[6]

Breach of Confidentiality and Privacy: The ITA prohibits the disclosure of information that is obtained without consent of the relevant individual.[viii]

Regulations for Intermediaries: The Intermediaries due diligence requirements are provided in the Information Technology (Intermediary Guidelines) Rules, 2011 ("**Intermediary Guidelines**") and lay down the regulations for intermediaries to follow concerning the content that passes through their systems. The rules also establish what content is and is not allowed to be posted by individuals, and holds intermediaries responsible for ensuring that websites are in compliance with the provisions.

Regulations for Cyber Café: The Information Technology (Guidelines for Cyber Café) Rules, 2011 provide regulations for the maintenance of user records by cyber cafés. Critical information under the Rules includes forms of identification and user browsing information.

Encryption Standards: There are two places in Indian law which lay down regulations for encryption in India. The ITA, provides the Central Government with the power to set the nationally permitted standard for encryption.[ix] The Internet Service Providers License, currently sets this limit at 40 bit (even though the ISP License is issued under the Telegraph Act, 1885 and not the ITA.[x] Additionally, the ISP License restricts service providers from employing bulk encryption of their networks, and requires that any individual or entity using encryption over 40 bit must seek permission from the Department of Telecommunications and deposit the key with the Department.

Electronic Service Delivery: In April 2011 the Electronic Service Delivery Rules to the Information Technology Act[xi] were notified. The Rules enable state governments to deliver public services through electronically enabled kiosks and other electronic service delivery mechanisms. In doing so the Rules maintain that state governments must create a system for the electronic delivery of services, and the appropriate authorities must create and maintain repositories of electronically signed records

[6] ITA section 67B

Interception of Communications: The interception powers laid out in the ITA were amended in 2008, and in 2009 the *IT Procedure and Safeguards for Interception, Monitoring, and Decryption of Information Rules*, 2009 ("**IT Interception Rules**") were notified.

Monitoring and Collection of Traffic Data: The collection and monitoring of traffic data is legalized through rules notified under 69B.

Provisions in the ITA that relate to the privacy principles include:

Oversight

- *Monthly Reporting for Cyber Cafes:* The cybercafé must submit hard and soft copies of the monthly report of the log register by the 5th day of every month to the person or agency specified by the Department of Telecommunications.[xii]

- *Inspection of Cyber Cafes:* Any officer authorised by the registration agency may check and inspect any cybercafé and the computer resource or established network at any point of time for the purpose of ensuring compliance. The cybercafé owner must provide every related document, register, and necessary information to the inspecting officer on demand.[xiii]

  This provision dilutes individual privacy as there are no safeguards such as court order, official rank, and specified circumstance to protect against undue access to information by law enforcement.

- *Investigatory powers for the Controller:* The ITA creates the Controller of Certifying Authorities, who is responsible for a number of functions including, but not limited to: supervising the activities of the Certifying Authorities, certifying public keys of the Certifying Authorities, laying down standards for Certifying Authorities. When section 28 is read with the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 the CCA is empowered to obtain information from any company or body corporate. According to the statute, the body corporate is required to give the information to the CCA or be penalized under section 44 (a).[xiv] [7]The Controller or any officer authorized by him, will have the power to undertake investigation of any contravention of the provisions of the ITA.[xv] The Controller or any person authorized by him shall, if he has reasonable cause to suspect that any contravention of the provisions of Chapter 6 (Regulation of Certifying Authorities) of the ITA, Rules or Regulations has been committed, have access to any computer system, any apparatus, data or any other material connected with such system, for the purpose of searching and obtaining any data contained in or available to such computer system. Furthermore, the Controller or

---

7 To find out the extent to which information has been requested by agencies through the CCA, the Software Freedom Law Center sent an RTI to the Controller of Certifying Authority. Among other responses, the CCA stated that 73 notices were issued by the CCA under section 28 of the ITA, in the last three years. The reply further stated that the notices were issued to Yahoo India, Google, AOL, Facebook, Orkut and Hotmail.[7]

any person authorized by him may, by order, direct any person in charge of, or otherwise concerned with the operation of, the computer system, to provide him with such reasonable technical and other assistance as he considers necessary.[xvi]

- *Competent Authority to authorize interceptions:* 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 "competent authorities" to issue interception directions.[xvii] In unavoidable circumstances the Joint Secretary to the Government of India, when so authorised by the Competent Authority, may issue an order. In further cases of emergency the interception, monitoring, or decryption of information may be carried out with approval from the head or the second most senior officer of the security and law enforcement agency at the central level and an authorised officer at or above the rank of police inspector general of or equivalent at the state or union territory level.[xviii] According to the 2008 amendment, the Central Government or State Government, or any of its officers specially authorised, may issue directions for interception.xix According to the unamended 2000 statute, only the Controller, who was an individual empowered by the Central Government, was given the authority to give direction for interception.xx The IT Interception Rules serve as a dilution from the original 2000 statute, as they appoint multiple authorities capable of issuing interception orders at the State level and in unavoidable circumstances.

- *Agencies of the government to intercept:* 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 ITA.[xxi] The IT Interception Rules further provide that the competent authority may give any decryption direction to the decryption key holder.[xxii]

- *Review committee to validate interception directions:* Every two months, a review committee is required to meet and record its findings as to whether the direction is valid. If the review committee is of the opinion that it is not, it can set aside the direction and order the destruction of all information collected.[xxiii] A copy of every direction issued by the competent authority must be forwarded to the review committee within a period of seven working days.[xxiv]
- *Nodal officer to authenticate directions:* The agency authorised by the Secretary of Home Affairs will 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.[xxv]
- *List of interception orders:* Every fifteen days the officers designated by the intermediaries are required to forward to the nodal officer in 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. [xxvi]

Accountability

- *Interception Orders*:

- *No interception order without permission of competent authority:* Every act of interception, monitoring or decryption of any information generated, transmitted, received or stored in any computer resource shall require an order of approval issued by the competent authority.[xxvii]
- *Information required in interception order*: 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.[xxviii]
- *Reasons for interception*: 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.[xxix]
- *Consideration of alternate means:* 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.[xxx]
- *Period for interception directions to stay in force*: 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. [xxxi]
- *Interception in case of emergencies:* Any approved interception order in the case of an emergency must be communicated to the competent authority within three days of its issue, and approval must be obtained from the authority within seven working days. Failing that, the order lapses.[xxxii]
- *Interception beyond jurisdiction*: 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.[xxxiii]
- *Agency officer to issue order to nodal officer:* The officer of the security agency issuing an order for interception is required to issue requests in writing to designated nodal officers of the service provider.[xxxiv]
- *Provision of facilities and assistance:* 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.[xxxv] Additionally, decryption key holders are required to disclose the decryption key and provide assistance in decrypting information for authorized agencies.[xxxvi]

  Though the 2000 statute required a subscriber,[8] intermediary or any person in charge of a computer resource to extend assistance and facilities and technical assistance to decrypt information[xxxvii], the 2008 Amendment expanded these orders by requiring the above.

Openness

- *Mandatory privacy policy for intermediaries:* All intermediaries are required to publish a mandatory privacy policy and user agreements.[xxxviii] The intermediary must inform its users that in the case of non-compliance with the

[8] "Subscriber" means a person whose name the Electronic Signature Certificate is issued. Section 2(zg) of the ITA 2000

established rules and regulations, the intermediary has the right to terminate the access or usage rights of the user and remove non-compliant information.[xxxix]

Security

- *Security protocol for intermediaries*: Intermediaries are required to provide any authorised governmental agency with information that is requested in writing for the purpose of: verification of identity; the prevention, detection, investigation, and prosecution of cyber security incidents; and punishment under any law currently in force.[xl]

  The broad reasons for which law enforcement are permitted to access information, particularly for the purpose of verifying identity could be used to facilitate tracking and invasion of privacy.

- *Security protocol for cyber cafes:* Cybercafés must take all precautions necessary to ensure that their computer systems are not used for illegal activities.[xli] This includes having in place safety/filtering software so as to prevent access to web sites relating to pornography, obscenity, terrorism, and other objectionable materials.[xlii]

- *Physical layout in cyber cafes:* Cybercafés must install partitions that are no higher than four and half feet and all screens must be installed to face outward. Additionally, the screens of all computers other than those situated in partitions or cubicles, must face outward into the common open space of the cybercafé. [xliii]

  This requirement serves to detract from the physical privacy of cyber cafe users, as it is not possible to use a computer without one's screen being open to viewing by other users.

- *Encryption of sensitive records held by companies delivering services electronically*: The appropriate government is allowed to determine the manner of encryption and confidentiality for sensitive electronic records while they are electronically signed.[xliv]
- *Security procedures for maintenance of electronic data held by companies delivering services electronically:* The appropriate government must specify the security, management, and storage procedures for maintenance of electronic data, information, applications etc. stored in the repository by companies delivering services electronically.[xlv]
- *Internal checks to prevent unauthorized interception:* The service provider must put in place adequate internal checks to ensure that unauthorised interception does not take place, and to ensure that secrecy of intercepted information is maintained.[xlvi] This includes ensuring that the interception and related information are handled only by the designated officers of the service provider.[xlvii]

Disclosure

- *Surveilled material to be disclosed only for intended purpose:* 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 and to the intended recipient.[xlviii]

- *Prohibition of unauthorized disclosure for companies providing the electronic delivery of services:* All companies providing services electronically must submit a declaration stating that the data of every individual transaction and citizen will be protected. If unauthorized disclosure without consent takes place, the service provider will be debarred from providing that service any further.[xlix]

- *Required disclosure to law enforcement by intermediary:* Intermediaries are required to provide any authorised governmental agency with information relating to the removal of content prohibited under the ITA, that is requested in writing for the purpose of: verification of identity; the prevention, detection, investigation, and prosecution of cyber security incidents; and punishment under any law currently in force.[l]

  The broad reasons for which law enforcement are permitted to access information, particularly for the purpose of verifying identity could be used to facilitate tracking and invasion of privacy.

- *Required Disclosure for companies providing the electronic delivery of services:* Records maintained by Service Providers must be disclosed to any agency or person nominated by the appropriate government for inspection and audit.[li]

- *Disclosure of intercepted material by security agencies*: Authorised 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. lii

Purpose Limitation

- *Prohibition of content to be hosted by intermediary*: Among other content, individuals are not allowed to host, display, upload, modify, publish, transmit, update or share information that:

  - Belongs to another person and to which the user does not have any rights;
  - Is grossly harmful; harassing; blasphemous; defamatory; obscene; pornographic; pedophilic; libellous; invasive of another's privacy; hateful or racially/ethnically objectionable; disparaging; related to money laundering; harmful to minors;
  - Violates another’s intellectual property rights or any law in force;

- Is deceptive or misleading; impersonates another;
- Contains software viruses or any other computer code designed to interrupt, destroy, or limit the functionality of a computer resource .[liii]

If a notice is served to an intermediary concerning prohibited information under the ITA, the intermediary must respond within 36 hours.[liv]

This provision could potentially serve to protect the privacy of individuals, as it prohibits content that is privacy infringing, and could be used by individuals to take down personal information, yet the broad terminology also places the freedom of expression at risk.

- *Surveillance for specified purposes*: Any authorised agency or body is permitted to intercept, monitor, or decrypt information that is generated, transmitted, received, or stored in any computer resource for the specified purpose.lv

  These permitted actions originate from the 2008 amendment, lvi but diverge from the 2000 statute, which originally provided for only the interception and decryption of information that was transmitted from any computer resource.lvii Thus, the 2008 amendment has expanded surveillance in two ways: 1. by additionally allowing for the monitoring of any information 2. by allowing for surveillance on information that is generated, transmitted, received, or stored in any computer resource– rather than information that is only transmitted.

- *Permitted conditions for surveillance:* Conditions in which interception, monitoring, and decryption is permitted include: in the interest of the sovereignty or integrity of India, the defence of India, the security of the state, friendly relations with foreign states, or public order, or to prevent incitement to the commission of any cognizable offence relating to the same, or for investigation of any offence.[lviii]

  Of these, the 2008 amendment added ‘defense of India’ and ‘or for investigation of any offence', and the competent authority may additionally issue directions to any agency of the government to monitor and collect traffic data for a range of “cyber security” purposes including, *inter alia*, “identifying or tracking any person who has breached, or is suspected of having breached or being likely to breach, cyber security”.[lix] Thus, the 2008 amendment expanded the circumstances for interception, monitoring, and decryption.

Collection Limitation

- *Retention of Information by Intermediaries***:** Any information removed by the intermediary upon notice will be preserved for a period of 90 days for the purposes of investigation.[lx]

This provision is a potential threat to privacy because of the large amount of (sensitive) information that could be taken down, stored by the intermediaries, and used by law enforcement agencies.

- *Retention of records by Cyber Cafes*: Cybercafés must record, maintain and prepare four types of records:
    - Copies of identity documents which have either been scanned or photocopied are to be maintained securely for a period of one year.[lxi]
    - A log register containing the required information[9] for a period of one year.[lxii] Online copies of the log register are to be maintained and must be authenticated with an electronic or digital signature.[lxiii]
    - Cybercafés must also prepare a monthly report of the log register showing dated details on the usage of their computer systems that is to be submitted to the person or agency as directed by the registration agency [lxiv]
    - The cybercafé owner must store and maintain backup register logs for at least six months. These logs must include:
        - ✓ history of websites accessed using computer resource at cyber cafe
        - ✓ logs of proxy servers installed at cyber café.[lxv]

- *Mandated proof of identity at Cyber Cafes:* The rule establishes seven acceptable forms of identification, at least one of which must be presented before an individual is allowed to use the cyber café's facilities.[10] In addition, the individual may also be photographed for establishing his/her identity. All children must also carry a proof of identity or be accompanied by an adult when using a cybercafé.[lxvi]

- *Data Retention of licenses and permits by companies electronically delivering services***:** All authorities that issue a license, permit, certificate etc. must create a repository of the signed records and retain these records. The manner in which these documents must be retained will be established by the appropriate government.[lxvii] Additionally, the appropriate government has the authority to direct any service provider to retain records of the transactions, receipts, and vouchers collected from payments.[lxviii]

- *Destruction of interception records:* All records, including electronic records, pertaining to interception must be destroyed by the government agency every six months, except when required for functional purposes.[lxix] 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.[lxx]

Notice

---

9 Required information includes: Name, address, gender, contact number, type and detail of identification document, date, computer terminal identification, log in time, log out time.

10 Acceptable forms of identity include: 1. Identity card issued by any School or College, 2. Photo Credit Card or debit card issued by a Bank or Post Office 3. Passport 4. Voter identity cad 5. Permanent Account Number (PAN), Photo Identity Card issued b y the employer or any Government Agency 6. Driving license issued by the Appropriate Government 7. UID number issued by UIDAI

- *Notice of non-compliance with terms*: The intermediary must provide notice to users that in the case of non-compliance with the provisions of the Rules, user agreement and privacy policy, the intermediary has the right to take down non-compliant information and prevent access to the information.[lxxi]

  This provision of notice is limited in many ways. Most importantly, intermediaries are not required to provide notice that content has been taken down, and the Rules do not require that users are notified of the presence of cookies and do-not track options.

Quality/Verification

- *Verification of changes to records held by companies delivering services electronically:* All changes made to records held by companies delivering services electronically, held in a repository, including updating or correcting the record, must be signed by the person authorized to make the changes along with time stamps of the original creation and modification. [lxxii]

Penalty/Offenses/Liability/Remedy

- *Grievance Officer for complaints pertaining to content online hosted by intermediaries***:** The intermediary must publish the name and contact details of the grievance officer as well as mechanism by which users can notify their complaints. The grievance officer must redress the complaints within one month of the date the complaint was received. [lxxiii]

  Though the provision of a grievance mechanism protects privacy it does not provide for any compensation to be paid to the aggrieved individuals whose privacy was infringed for before the information was taken down.

- **Hacking**

Offense	**Fine**	**Imprisonment**
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.[lxxiv]	Damages upto 1 crore	

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.[lxxv]		Imprisonment for life

- **Voyeurism**

Offense	**Fine**	**Imprisonment**
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[lxxvi]	Not exceeding two lakh rupees	Up to three years

- **Child Pornography**

Offense	**Fine**	**Imprisonment**
The publication or transmission of explicit or sexual material pertaining to children in an electronic form is prohibited. Any person who creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges, or distributes material in any electronic form that depicts children in a sexually explicit manner, cultivates entices or induces children to online relationship with one or more children for a sexually explicit act, facilitates abusing children online, or records in electronic form sexual abuse of children.	May extend to ten lakh rupees	Five Years [lxxvii]

- **Breach of Confidentiality and Privacy**

Offense	**Fine**	**Imprisonment**
Disclosure of information accessed without consent.[lxxviii]	May extend to one lakh rupees	Up to two years

- **Disclosure of information in breach of lawful contract**

Offense	Fine	Imprisonment
Disclosure of information by a person or intermediary with the intent of causing wrongful loss or wrongful gain, without the consent of the person concerned, or in breach of a lawful contract.[lxxix]	May extend to five lakh rupees	Up to three years

- **Interception**

Offense	Fine	Imprisonment
Service providers that do not comply with interception requests from authorised agencies.	Amount not specified	Seven years [lxxx]
Intermediaries or any 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	May extend to one lakh rupees	Two years lxxxi

Missing Principles:

- **Choice and Consent**
- **Access and Correction**

Case Law: Information Technology Act 2000

Shashank Shekhar Mishra v. Ajay Gupta[11]

In the case of *Shashank Shekhar Mishra* v. *Ajay Gupta*, Delhi High Court, 5-09-2011 Shashank Shekhar's laptop was stolen along with all the data in it when the defendant, barged into Shashank's premises and snatched his laptop, which contained confidential and personal information including vital financial data relating to the bank account of his mother and credit card account of his cousin, all of which had the potential of being misused as well as personal messages and private photographs. The Court recognized the limitations of Section 43 of the ITA, which provides penalty for damaging a computer or computer system, and held that in this case, where the laptop was snatched and contained personal and confidential information, the civil court has the right to award damages, despite section 61 of the ITA which requires that when possible, cases must be heard only by the Cyber Appellate Tribunal constituted under the Act. Discussing this issue the High Court held:

[11] http://www.indiankanoon.org/doc/58657750/

"9. Coming to damages, as noted earlier, the laptop stolen by the defendant contained vital and important data as also the computer programme authored by [Shashank] ……..The plaintiff must have suffered a lot of mental agony and anxiety on account of theft of the computer programme authored by him as well as all important data which was stored in the laptop. He would always remain apprehensive and live under a constant fear that the data which he had stored in the laptop may be misused either by the defendant or any other person who is able to have access to it, causing substantial financial loss to him besides mental trauma, agony and anxiety, which he is bound to suffer in case that data is used. The anxiety and mental trauma of the plaintiff on account of his being deprived of the work authored by him needs to be appreciated taking into consideration the tremendous effort which he must have made in developing that computer programme.

11. Though Section 43 of the Information Technology Act, 2000 provides for payment of damages by way of compensation in case of theft of a computer source Code……., it does not provide for payment of damages for theft of any other type of data other than computer source Code used for a computer resource. Hence, the jurisdiction of a Civil Court is not excluded under Section 61 of the Act."

In its final decision the Court proceeded to award the plaintiff exemplary damages of Rs. 10 lakh, which is a significant amount of compensation for mental agony. The court also discussed how the defendant's actions violated the privacy of the plaintiff:

"8. ……..The privacy of the plaintiff has already been invaded by the defendant snatching the laptop containing the above-referred private information since he thereby had access to that private information of the plaintiff. The defendant has no right to part with that information to any person and thereby give them an opportunity to invade the privacy of the plaintiff. The plaintiff, therefore, is entitled to an injunction restraining the defendant from parting with the aforesaid information to any person as also from using it in any manner."

Case Highlights

Because section 43 of the Information Technology Act 2000 only provides for damages in case of theft of computer source code, it does not take away the power of a court to award damages for mental agony, etc. caused by the theft of a laptop containing personal and sensitive information.

K.N. Govindacharya v. Union of India[lxxxii]

There are a number of criticisms of the Intermediary Guidelines such as the lack of an independent authority to judge whether the content is objectionable before taking it down, shifting of the burden to prove that the content is damaging on the person putting up the content rather than the person alleging that its objectionable, shifting the blame on the intermediaries for third party content, lack of proportionality, vague requirements and standards, etc. Another problem with the Intermediary Guidelines stems from Section 1(2) of the Information Technology Act, 2000 which makes the Act applicable to "any offence or contravention thereunder committed outside India by any person" thereby giving it extra-territorial jurisdiction, i.e. makes this Indian law applicable to people outside India as well, whether they are Indians or foreigners. The implications of this extra territorial jurisdiction came to the fore in a recent interim order dated August 23, 2013 in a Public Interest Litigation (PIL) *K.N. Govindacharya* v. *Union of India*,[lxxxiii] where the Hon'ble Delhi High Court held that even websites such as Google and Facebook will have to comply with the Intermediary Guidelines since they fall within the definition of the term "Intermediary".

However the implications of applying such onerous obligations on non Indian citizens are not discussed anywhere in the order. This could mean that the Intermediary Guidelines can possibly be applied to any website which is accessible from India irrespective of who runs it, from where or for what purpose. Furthermore in the same PIL it was urged by the petitioners that minors should not be allowed to open facebook and orkut accounts since they are not allowed to enter into contracts. The Court agreed with this argument and held that:

"there is no dispute that children below the age of 13 years are not permitted to open such accounts. It is not in dispute that if it comes in the knowledge of any person that a child below the age of 13 years has opened such an account he may make a complaint to the social networking site who shall then take appropriate action, after verification, for deletion of that account."

On the other hand the websites have argued that not allowing minors to open accounts would limit their right to freedom of speech and expression. The PIL is still pending in the Delhi High Court and a final decision on this issue is yet to be taken.

Case Highlights

The provisions of the Information Technology Act apply to citizens and non citizens. This could possibly protect privacy of foreigners, by extending privacy protections under the act to foreigners, but could also dilute privacy by permitting governmental access to foreign data.

Indian Telegraph Act 1885

The Indian Telegraph Act, 1885 (**TA**) was passed to govern telegraphy, phones, communication, radio, telex and fax in India. The Act allows any authorized public official to intercept communications.[lxxxiv] In 2007 interception rules were issued under Rule 419 of the Indian Telegraph Rules. The TA allows any authorized public official to intercept telephonic communications. Provisions that relate to the privacy principles include:

Oversight

- *Authorization of Interception Orders:* Interception may only be authorised by the Secretary of the Ministry of Home Affairs in the case of the Central Government and the Secretary of the Home Department in the case of the State Government or an officer at or above the rank of a Joint Secretary, who has been authorised by the Union Home Secretary.[lxxxv]
- *Approval of interception orders for emergent cases:* In the case of remote areas or where for operational reasons obtaining directions for interception is not feasible, interception will take place with authorisation from the head or the most senior officer of the security agency at the Central level or officers not below the rank of Inspector General of Police.[lxxxvi] For emergent cases, the tapping order must be sent to the competent authority for approval within three days. If the order is not approved within seven days, the interception must cease.[lxxxvii]
- *Constitution of a Review Committee:* The review committee should be constituted of: a Cabinet Secretary, Secretary to the Government of India incharge Legal Affairs, Secretary to the Government of India of the Department of Telecommunications. At

the State level, the review committee must consist of: Chief Secretary, Secretary Law, Secretary to the State Government other than the Home Secretary.[lxxxviii]

Accountability

- *Chain of Custody for Interception:*

    - *Designated authorities in security agencies to send interception orders*: All security agencies must designate an official not below the rank of Superintendent of Police to authenticate and send interception orders to the designated officers of the service providers.[lxxxix]
    - *Orders to be sent to review committee:* A copy of every order issued by the competent authority must be sent to the review committee within seven working days.xc
    - *Designated officer to convey interception order*: Directions for interception must be conveyed to the designated officer of the service provider by an officer not below the rank of Superintendent of Police or Additional Superintendent of Police or the officer of the equivalent rank.[xci]
    - *Designated officer of service provider to handle interception orders:* The service provider must designate two senior officers in every licensed service area as nodal officers to receive and handle interception orders.[xcii]
    - *Service provider officer to maintain records:* The designated officer authorized to intercept any message must maintain records including: the intercepted message, the particulars of the person whose message was intercepted, the name and details of the officer who intercepted the message, the number of copies that were made of the message, the mode and method of the copies made, and the date of destruction of the copies, and the duration within which the orders remain in force.xciii
    - *Service provider officer to acknowledge receipt of interception order:* The officers appointed by the service providers must acknowledge the receipt of an order for interception within two hours of receiving the order.[xciv] Every 15 days the nodal officer of the service provider must forward a list of interception authorisations to the nodal officers to confirm its authenticity. The list must include the date of the orders, the date and time of receiving the orders, and the date and time of implementation.xcv

Security

- *Internal checks:* Service providers must put in place internal checks to ensure that unauthorized interceptions of messages do not take place and the secrecy of messages is maintained.[xcvi]
- *Handling of intercepted messages:* Service providers must ensure that intercepted messages are only handled by the appointed nodal officer.xcvii

Disclosure

- *Specified disclosure required*: The interception order should specify the name and the designation of the officer of the authority to whom the intercepted message will be disclosed to and the use of the intercepted message.xcviii

Purpose Limitation

- *Circumstances for Interception:* Communications can be intercepted under the TA during public emergencies or in the interest of public safety provided that certain other

grounds also apply, namely, such interception is in the interest of sovereignty and integrity of India, the security of the State, friendly relations with foreign states, public order and the prevention of incitement of offences.xcix

- *Reasons for interception to be stated:* Interception orders must contain the reasons for the order.[c]
- *Specific interception orders:* Interception orders must describe a specific individual and specific address or premises. ci
- *Duration of Interception Order:* Each order unless, canceled earlier, is only valid for 60 days and can only be extended to a maximum of 180 days.cii

Collection Limitation

- *Other means for collection:* While issuing directions for interception the competent authority must determine if it is possible to obtain the information through other means.[ciii]
- *Destruction by security agencies:* Records of directions for interception must be destroyed every six months by the relevant competent authority and the authorized security and Law Enforcement Agencies – unless they are required for 'functional requirements'.civ
- *Destruction by Service Providers:* Service providers must destroy records pertaining to directions for interception within two months of discontinuing the interception.cv

Quality/Verification

- *Review committee to validate legality of wiretap:* A review committee is to meet every two months at the central/state level and must validate the legality of the wiretap. When the review committee finds that an order is not legal, they may set aside the order and have any intercepted messages destroyed. [cvi]

Liability/Remedy Penalty/Offenses

- *Liability***:** Service providers are to be held responsible for the actions of their employees, and if a violation of the IT Rules takes place, action will be taken against the service provider.cvii
- *Unauthorized Interception*

Offense	**Fine**	**Penalty**
Unauthorized interception	Amount not specified	Imprisonment for up to three years. cviii

Missing Principles

- Choice and Consent
- Access and Correction
- Openness

Notice

Case Law: Indian Telegraph Act 1885

People's Union for Civil Liberties v. Union of India[12]

It is interesting to note here that although the power of interception had always existed under the Telegraph Act, no rules or regulations were prescribed regarding the procedure to be followed for interception nor any safeguards were laid down. This issue was taken note of by the Supreme Court in the case of *People's Union for Civil Liberties* v. *Union of India*,[13] Supreme Court of India, 18-12-1998 which is one of the most influential cases in the entire privacy paradigm because it was due to the efforts of the Supreme Court in this case that the Central Government issued Rules under the Telegraph Act, 1885 regarding interception of communications.. It is also significant that the principles and safeguards developed in this case have been followed in most Indian legislations regarding interception of communications ever since. Discussing the right to privacy, the Supreme Court in the *PUCL case* held:

"Telephone - Tapping is a serious invasion of an individual's privacy. With the growth of highly sophisticated communication technology, the right to hold telephone conversation, in the privacy of one's home or office without interference, is increasingly susceptible to abuse. It is no doubt correct that every Government, howsoever democratic, exercises some degree of subrosa operation as a part of its intelligence outfit but at the same time citizen's right to privacy has to be protected from being abused by the authorities of the day.

The right privacy - by itself - has not been identified under the Constitution. As a concept it may be too broad and moralistic to define it judicially. Whether right to privacy can be claimed or has been infringed in a given case would depend on the facts of the said case. But the right to hold a telephone conversation in the privacy of ones home or office without interference can certainly be claimed as "right to privacy". Conversations on the telephone are often of an intimate and confidential character. Telephone conversation is a part of modern man's life. It is considered so important that more and more people are carrying mobile telephone instruments in their pockets. Telephone conversation is an important facet of a man's private life. Right to privacy would certainly include telephone-conversation in the privacy of one's home or office. Telephone-tapping would, thus, infract Article 21 of the Constitution of India unless it is permitted under the procedure established by law.

Right to freedom of speech and expression is guaranteed under Article 19(1) (a) of the Constitution. This freedom means the right to express ones convictions and opinions freely by word of mouth, writing, printing, picture, or in any other manner. When a person is talking on telephone, he is exercising his right to freedom of speech and expression. Telephone-tapping unless it comes within the grounds of restrictions under Article 19(2) would infract Article 19(1)(a) of the Constitution."

It is interesting to note that in *People's Union for Civil Liberties* v. *Union of India*,[14] Supreme Court of India, 18-12-1998 the Supreme Court also discussed the meaning of the term "public emergency" under section 5(2) of the Telegraph Act noting that:

---

[12] http://www.indiankanoon.org/doc/87862/
[13] http://www.indiankanoon.org/doc/87862/
[14] http://www.indiankanoon.org/doc/87862/

"26. Learned counsel assisting us in this case have not seriously challenged the constitutional vires of Section 5(2) of the Act. In this respect it would be useful to refer to the observations of this Court in Hukam Chand Shyam Lal vs. Union of India & Ors. 1976 (2) SCC 128:-

28. Section 5(2) of the Act permits the interception of messages in accordance with the provisions of the said Section. "Occurrence of any public emergency" or "in the interest of public safety" are the sine qua non for the application of the provisions of Section 5(2) of the Act. Unless a public emergency has occurred or the interest of public safety demands, the authorities have no jurisdiction to exercise the powers under the said Section. 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 exercise, 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 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 public order or for preventing incitement to the commission of an offence, it cannot intercept the messages 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."

At the end the Supreme Court laid down various safeguards to be followed before an order for interception could be passed under the Telegraph Act and these directions were later adopted and incorporated into the interception rules promulgated by the ministry by way of an amendment to the Telegraph Rules, which we shall discuss below.

State of Maharashtra* v. *Bharat Shanti Lal Shah and others[15]

As mentioned above, the safeguards for the interception provisions in most legislations in India follow the directives laid down by the Supreme Court in *PUCL*'s case and incorporated in the Telegraph Rules. This is also true of anti-terrorism legislations such as the Maharashtra Control of Organized Crime Act, 1999 (MCOCA) which contain interception provisions in Sections 13 to 16. The legislative competence of the state to enact these provisions was challenged in front of the Supreme Court in the case of *State of Maharashtra* v. *Bharat Shanti Lal Shah and others*,[16] 1-9-2008. The Supreme Court while deciding on the constitutional validity of the impugned sections, observed that though the interception of communications is an invasion of an individual's right to privacy, the right to privacy is not absolute, thus the court is required to see that the procedure itself is fair, just, and reasonable. In the case, the Court held:

"44. The interception of conversation though constitutes an invasion of an individual right to privacy but the said right can be curtailed in accordance to procedure validly established by

[15] http://indiankanoon.org/doc/698472/
[16] http://indiankanoon.org/doc/698472/

law. Thus what the Court is required to see is that the procedure itself must be fair, just and reasonable and non arbitrary, fanciful or oppressive.

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

Interception provisions also exist in some of the more significant anti crime and anti terror legislations in India such as the Terrorist and Disruptive Activities (Prevention) Act, 1987, the Maharashtra Control of Organised Crimes Act, 1999, the Prevention of Terrorism Act, 2002, etc. These provisions lay down the conditions as well as safeguards required for legal and lawful interception of telecommunications and also deal with the evidentiary and investigative value of such intercepted conversations. In the case of *State (N.C.T. of Delhi)* v. *Navjot Sandhu @ Afsan Guru*[cix] (*Afsan Guru case*) the Supreme Court of India considered the legality and validity of intercepted conversations in the following manner:

"The legality and admissibility of intercepted telephone calls arises in the context of telephone conversation between Shaukat and his wife Afsan Guru on 14th December at 20:09 hrs and the conversation between Gilani and his brother Shah Faizal on the same day at 12:22 hrs. Interception of communication is provided for by the provisions contained in Chapter V of the POTO/POTA which contains Sections 36 to 48. The proviso to Section 45 lays down the pre-requisite conditions for admitting the evidence collected against the accused through the interception of wire, electronic or oral communication. Chapter V governing the procedure for interception and admission of the intercepted communications pre-supposes that there is an investigation of a terrorists act under the POTA has been set in motion. It is not in dispute that the procedural requirements of Chapter V have not been complied with when such interceptions took place on 14th December, 2001. But, as already noticed, on the crucial date on which interception took place (i.e. 14th December), no offence under POTA was included whether in the FIR or in any other contemporaneous documents. We have already held that the non- inclusion of POTO offences even at the threshold of investigation cannot be legally faulted and that such non-inclusion was not deliberate. The admissibility or the evidentiary status of the two intercepted conversations should, therefore, be judged de hors the provisions of POTO/POTA. On the relevant day, the interception of messages was governed by Section 5(2) of the Indian Telegraph Act read with Rule 419-A of the Indian Telegraph Rules. The substantive power of interception by the Government or the authorized officer is conferred by Section 5. The modalities and procedure for interception is governed by the said Rules. It is contended by the learned senior counsel appearing for the two accused Shaukat and Gilani, that even the Rule 419A, has not been complied with in the instant case, and, therefore, the tape- recorded conversation obtained by such interception cannot be utilized by the prosecution to incriminate the said accused. It is the contention of

learned counsel for the State, Mr. Gopal Subramanium, that there was substantial compliance with Rule 419A and, in any case, even if the interception did not take place in strict conformity with the Rule, that does not affect the admissibility of the communications so recorded. ***In other words, his submission is that the illegality or irregularity in interception does not affect its admissibility in evidence there being no specific embargo against the admissibility in the Telegraph Act or in the Rules. Irrespective of the merit in the first contention of Mr. Gopal Subramanium, we find force in the alternative contention advanced by him.***

In regard to the first aspect, two infirmities are pointed out in the relevant orders authorizing and confirming the interception of specified telephone numbers. It is not shown by the prosecution that the Joint Director, Intelligence Bureau who authorized the interception, holds the rank of Joint Secretary to the Government of India. Secondly, the confirmation orders passed by the Home Secretary (contained in volume 7 of lower Court record, Page 447 etc.,) would indicate that the confirmation was prospective. We are distressed to note that the confirmation orders should be passed by a senior officer of the Government of India in such a careless manner, that too, in an important case of this nature. However, these deficiencies or inadequacies do not, in our view, preclude the admission of intercepted telephonic communication in evidence. It is to be noted that unlike the proviso to Section 45 of POTA, Section 5(2) of the Telegraph Act or Rule 419A does not deal with any rule of evidence. The non-compliance or inadequate compliance with the provisions of the Telegraph Act does not per se affect the admissibility. The legal position regarding the question of admissibility of the tape recorded conversation illegally collected or obtained is no longer res integra in view of the decision of this Court in R.M. Malkani v. State of Maharashtra, [(1973) 1 SCC 471]. In that case, the Court clarified that a contemporaneous tape record of a relevant conversation is a relevant fact and is admissible as res gestae under Section 7 of the Evidence Act."

Thus is seems from the above that the Supreme Court is of the view that even if the procedure prescribed under the Telegraph Act and Rules for interception of conversations is not followed even then the intercepted communications would be admissible in evidence since the Telegraph Act and the Rules thereunder do not lay down any rule regarding the evidentiary value of illegally intercepted communications.

Case Highlights

- Interception of conversation, though constitutes an invasion of individual privacy, this right can be curtailed in accordance with procedure validly established by law.

- This procedure for intercepting communications must be fair, just and reasonable and not arbitrary, fanciful or oppressive.

Comparison of interception provisions under ITA and TA:

Comparison of the interception rules found under the TA and the ITA show that interception in the ITA has been expanded in the following ways:

- **Grounds for interception***:* The TA creates two levels of circumstances that must met before the interception of communications can take place: 1. A public emergency must be in force or in the interest of public interest or safety 2. If the former is satisfied, interception may take place if it is found to be in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order, or for preventing incitement to the commission of an offence. The ITA expands these powers by removing the condition of 'public emergency, public interest, public safety' and allowing for interception to additionally take place for the investigation of any offence.
- **Types of interception***:* The ITA allows for the interception, monitoring, and decryption of information,[cx] while the TA allows only for the interception of communications.[cxi]
- **Types of information:** The ITA allows for the interception of information that is generated, transmitted, received or stored in a computer resource[cxii], while the TA allows for interception of information from any message or class of message brought for transmission by or transmitted or received by any telegraph.[cxiii]
- **Provision of facilities:** The ITA requires that intermediaries must provide all facilities, co-operation, and assistance for the interception, monitoring, or decryption of information.[cxiv] Such a requirement is not found in the TA.
- **Disclosure of decryption key***:* The ITA requires that if requested by the nodal officer decryption key holders must disclose decryption keys and provide decryption assistance.[cxv] No such a requirement is found in the TA.
- **Intermediary to provide technical assistance:** The ITA requires that the intermediary must provide technical assistance and the equipment including hardware, software, firmware, stores, interface, and access to the equipment wherever requested for the purposes of installing interception equipment, maintaining interception equipment, removing interception equipment, or performing any action required for access to stored information.[cxvi] Such a provision is not found in the TA.
- **Destruction of records by service providers/intermediaries:** The ITA requires that the intermediary should destroy records pertaining to an interception within a period of two months of discontinuance unless required for an ongoing investigation, criminal complaint, or legal proceeding.[cxvii] Under the TA the service provider is required to destroy records two months after discontinuance of the interception order.[cxviii] Thus there does not seem to be any requirement on the service provider under the TA to keep the records beyond two months even if required for an ongoing investigation.

- **Security:** The ITA allows any person authorized by the service provider to access the communications system for the purpose of installing a computer resource, maintaining a computer resource, installing a communication link for the intermediary, accessing stored information relating to the maintenance etc. of the communication link, accessing or analyzing information from a computer resource for the purposes of: implementing information security practices, determining any security breaches, undertaking forensics as part of an investigation or audit, accessing information for the purpose of tracing a computer resource of someone who has contravened or is suspected of contravening the provisions of the Act.[cxix] An equivalent provision is not found in the TA.

- **Sharing with concerned agencies***:* Whenever asked by a concerned agency at the Central level, the state level agencies will share any information that they have obtained while following directions for interception.[cxx] An equivalent provision is not found in the TA.

- **Interception, monitoring, or decryption beyond the state jurisdiction:** If a State Gov. etc. requires interception beyond its jurisdiction the Secretary in charge of the Home Department will request permission from the Secretary of Ministry of Home Affairs.[cxxi]

Policies/Licences

In India interception powers are also given to the government through the Internet Services License (ISP) Agreement and the Unified Service Agreement License (UASL) for service providers. In practice, both licenses afford the government expansive access to communication data held and processed by service providers. It must be noted that since both the ISP and the UAS License Agreements are issued under the TA, technically the interception of messages under both these licenses can only be done if the conditions specified under the TA and the interception rules are satisfied. However, because of the additional obligations imposed upon the Service Provider under these licenses there is a very high risk of interception of messages in violation of the relatively stricter conditions enumerated in the TA and the interception rules issued under it since these additional obligations make the actual act of interception very easy for the authorities.

License Agreement for Provision of Internet Services

According to the Agreement for Provisions of Internet Services, the Government is afforded expansive access to communication data held by ISPs. Aspects that relate to the privacy principles include:

Oversight

- *Authorization for monitoring*: Monitoring shall only be by the authorization of the Union Home Secretary or Home Secretaries of the States/Union Territories.`cxxii
- *Types of access permitted to law enforcement, licensor, or authorized officials:*
    - *Access to log books by the licensor:* The licensor or its authority will have access to record files and logbooks stored by service providers.cxxiii
    - *Access to subscriber list by authorized intelligence agencies and licensor*: The complete and up to date list of subscribers will be made available by the ISP on a password protected website – accessible to authorized intelligence agencies.cxxiv Information such as customer name, IP address, bandwidth provided, address of installation, data of installation, contact number and email of leased line customers shall be included in the website.cxxv The licensor or its representatives will also have access to the Database relating to the subscribers of the ISP which is to be available at any instant.cxxvi

- *Circumstances for monitoring*:
    - *Right to monitor by the central/state government*: The designated person of the central/state government or the licensor or nominee will have the right to monitor telecommunications traffic in every node or any other technically feasible point in the network. To facilitate this, the ISP must make arrangements for the monitoring of simultaneous calls by the Government or its security agencies.cxxvii
    - *Right of DoT to monitor*: DoT will have the ability to monitor customers who generate high traffic value and verify specified user identities on a monthly basis.cxxviii

- *Inspections to be carried out:*
    - *Inspection of premises:* Periodic inspections will also be carried out on the premises of Internet leased line customers to check for possible misuse.cxxix
- *Right of the licensor to take over network:* The licensor has the right to take over the service equipment and networks of the ISP in the case of the public interest, national emergency, low intensity conflict, or any other reason when ordered to do so by the government.cxxx

Accountability

- *Provision of information by the ISP to defined authorities:*
    - *Provision of mirror images:* Mirror images of the remote access information should be made available online for monitoring purposes.cxxxi A safeguard provided for in the license is that remote access to networks is only allowed in areas approved by the DOT in consultation with the Security Agencies.cxxxii
    - *Provision of information stored on dedicated transmission link:* The ISP will provide the login password to DOT and authorized Government agencies on a monthly basis for access to information stored on any dedicated transmission link from ISP node to subscriber premises.cxxxiii
    - *Provision of location details of equipment provided*: The ISP will also provide the licensor with location details of the equipment provided by the ISP.cxxxiv
    - *Provision of subscriber identity and geographic location:* The ISP must provide the traceable identity and geographic location of their subscribers, and if the subscriber is roaming – the ISP should try to find traceable identities of roaming subscribers from foreign companies.cxxxv

- **Provision of facilities by ISP**
    - *Facilities for monitoring:* The ISP must provide the necessary facilities for continuous monitoring of the system as required by the licensor or its authorized representatives.cxxxvi
    - *Facilities for tracing*: The ISP will also provide facilities for the tracing of nuisance, obnoxious or malicious calls, messages, or communications. These facilities are to be provided specifically to authorized officers of the Government of India (police, customs, excise, intelligence department)

when the information is required for investigations or detection of crimes and in the interest of national security.cxxxvii

- *Facilities to counteract espionage*: ISPs should also provide facilities to the government from time to time to counteract espionage, subversive acts, sabotage or any other unlawful activity.cxxxviii
- *Facilities and equipment to be specified by government:* The types of interception equipment to be used will be specified by the government of India.cxxxix This includes the installation of necessary infrastructure in the service area with respect to Internet Telephony Services offered by the ISP including the processing, routing, directing, managing, authenticating the internet calls including the generation of Call Details Record, IP address, called numbers, date, duration, time, and charge of the internet telephony calls.cxl
- *Facilities for surveillance of mobile terminal activity*: The ISP must also provide the government facilities to carry out surveillance of Mobile Terminal activity within a specified area whenever requested.cxli
- *Facilities for monitoring international gateway:* As per the requirements of security agencies, every international gateway location having a capacity of 2 Mbps or more will be equipped will have a monitoring center capable of monitoring internet telephony traffic.cxlii
- *Facilities for monitoring in the premise of the ISP*: Every office must be at least 10x10 with adequate power, air conditioning, and accessible only to the monitoring agencies. One local exclusive telephone line must be provided, and a central monitoring center must be provided if the ISP has multiple nodal points.cxliii

- *Anonymous Access***:** Logins where the identity of the user is not known should not be permitted by the ISP.cxliv

Security

- *Protection of privacy*: There is a responsibility on the ISP to protect the privacy of its communications transferred over its network. This includes securing the information and protecting against unauthorized interception, unauthorized disclosure, ensure the confidentiality of information, and protect against over disclosure of information-except when consent has been given.cxlv

Collection Limitation

- *Records to be maintained and retained by ISP*
  - *Log of users:* Each ISP must maintain an up to date log of all users connected and the service that they are using (mail, telnet, http, etc). The ISPs must also log every outward login or telnet through their computers. These logs as well as copies of all the packets must be made available in real time to the Telecom Authority.cxlvi
  - *Log of internet leased line customers:* A record of each internet leased line customer should be kept along with details of connectivity, and reasons for taking the link should be kept and made readily available for inspection.cxlvii
  - *Log of commercial communications:* The ISP will maintain a record with regard to all commercial communications exchanged on the network.

These records must be archived for at least one year for scrutiny by the licensor or security agencies.cxlviii

- *Log of remote access activities:* The ISP will also maintain a complete audit trail of the remote access activities that pertain to the network for at least six months. This information must be available on request for any agency authorized by the licensor.cxlix

Missing Principles

- Choice and Consent
- Notice
- Quality/Verification
- Penalty/Offenses/Liability/Remedy
- Disclosure
- Access and Correction
- Purpose Limitation
- Openness

License Agreement for provision of Unified Access Services

Accountability

- Monitoring requirements: The ISP must make arrangements for the monitoring of the telecommunication traffic in every MSC exchange or any other technically feasible point, of at least 210 calls simultaneously.cl
- Records to be made available:
  - CDRS: When required by security agencies, the ISP must make available records of i) called/calling party mobile/PSTN numbers ii) time/date and duration of calls iii) location of target subscribers and from time to time precise location iv) telephone numbers – and if any call forwarding feature has been evoked – records thereof v) data records for failed call attempts vi) CDR of roaming subscriber.cli
  - Bulk connections: On a monthly basis, and from time to time, information with respect to bulk connections shall be forwarded to DoT, the licensor, and security agencies.clii
  - Record of calls beyond specified threshold: Calls should be checked, analyzed, and a record maintained of all outgoing calls made by customers both during the day and night that exceed a set threshold of minutes. A list of suspected subscribers should be created by the ISP and should be informed to DoT and any officer authorized by the licensor at any point of time.cliii
  - Record of subscribers with calling line identification restrictions: Furthermore, a list of calling line identification restriction subscribers with

their complete address and details should be created on a password protected website that is available to authorized government agencies.cliv

Collection Limitation

- *Provision of ID*: Mobile phone subscribers must register the SIM card that they are using.clv

Missing Principles

- Openness
- Oversight
- Security
- Disclosure
- Access and Correction
- Purpose Limitation
- Choice and Consent
- Notice
- Quality/Verification
- Penalty/Offenses/Liability/Remedy

Case Law

Amar Singh v. *Union of India and others*,[17]

In *Amar Singh* v. *Union of India and others*,[18] Supreme Court of India, 11-05-2011 the petitioner claimed that his privacy had been invaded by interception of his calls. The importance of this case lies in the fact that here the Supreme Court discussed the duties of a service provider when it receives an official request for interception, and held that if the request is full of procedural mistakes, then it is the duty of the service provider to simultaneously verify its authenticity while at the same time acting upon it. Discussing these duties the Court held:

"39. Therefore, while there is urgent necessity on the part of the service provider to act on a communication, at the same time, the [service provider] is equally duty bound to immediately verify the authenticity of such communication if on a reasonable reading of the same, it appears to any person, acting bona fide, that such communication, with innumerable mistakes, falls clearly short of the tenor of a genuine official communication. Therefore, the explanation of the service provider is not acceptable to this Court. If the service provider could have shown, which it has not done in the present case, that it had tried to ascertain from the author of the communication, its genuineness, but had not received any response or that the authority had accepted the communication as genuine, the service provider's duty would have been over. But the mere stand that there is no provision under the rule to do so is

[17] http://indiankanoon.org/doc/1082001/
[18] http://indiankanoon.org/doc/1082001/

a lame excuse, especially having regard to the public element involved in the working of the service provider and the consequential effect it has on the fundamental right of the person concerned.

40. In view of the public nature of the function of a service provider, it is inherent in its duty to act carefully and with a sense of responsibility. This Court is thus constrained to observe that in discharging the said duty, respondent No. 8, the service provider has failed.

41. Of course, this Court is not suggesting that in the name of verifying the authenticity of any written request for interception, the service provider will sit upon it. The service provider must immediately act upon such written request but when the communication bristles with gross mistakes, as in the present case, it is the duty of the service provider to simultaneously verify its authenticity while at the same time also act upon it. The Central Government must, therefore, frame certain statutory guidelines in this regard to prevent interception of telephone conversation on unauthorised communication, as has been done in this case."

Case Highlights

- Service provider is duty bound to verify the authenticity of a request for interception if on a reasonable reading it falls short of a genuine official communication.
- It is the duty of the service provider to act carefully and with a sense of responsibility.
- Service provider must immediately act upon a request for interception, but if it seems to be full of mistakes, should simultaneously verify its authenticity.

Rayala M. Bhuvaneswari v. *Nagaphanender Rayala*,[19]

Since the right to privacy is a fundamental right guaranteed by the State one might be tempted to ask whether it is at all possible to safeguard it against a non state actor or a purely private entity. This question was partially addressed by the case of *Rayala M. Bhuvaneswari* v. *Nagaphanender Rayala*,[20] Andhra Pradesh High Court, 20-12-2007 where in a matrimonial dispute, the Court discovered that the husband had tape recorded telephone conversation of his wife with her friends and parents, without her consent. Subsequently, he had been using this as evidence, in the divorce case between the parties. The Court held that the act of the husband was illegal and unconstitutional and infringing upon the privacy of the wife, and that even if the tapes are true, they cannot be admissible as evidence. Discussing the spouse's right to privacy the High Court held:

> *"3. ....There should be some trust between husband and wife and in any case, in my view, the right of privacy of the wife is infringed by her husband by recording her conversation on telephone to others and if such a right is violated, which is fundamental, can such husband, who has resorted to illegal means, which are not only unconstitutional, but also immoral, later on, rely on the evidence gathered by him by such means. Clearly, it must not be permitted."*

[19] http://www.indiankanoon.org/doc/1058685/
[20] http://www.indiankanoon.org/doc/1058685/

The Court then referred to various cases on the right to privacy and the right to order medical examination in matrimonial disputes and held:

> *"13. For all these reasons, I believe that the act of tapping itself by the husband of the conversation of his wife with others was illegal and it infringed the right of privacy of the wife. Therefore, these tapes, even if true, cannot be admissible in evidence. Hence, Ex.P-18 itself is not admissible in evidence and there is no question of forcing the wife to undergo a voice test and then ask the expert to compare the portions denied by her with her admitted voice."*

The importance of this case lies in the fact that the Court has acknowledged that the protection of the right to privacy under Article 21 of the Constitution of India is not only enforceable against the State but also against individuals including their own spouses.

Case Highlights

- Tapping the phone of the spouse without consent is illegal and an infringement of the spouse's right to privacy. Information that is collected through the illegal interception of communications cannot be used as evidence in a court of law.

TRAI Regulations on Unsolicited Marketing Calls

Unsolicited telemarketing calls and text messages, which are sent in bulk pose a threat to privacy, because besides causing disturbance and irritation, bulk text messaging can be used as a tool for phishing. For many years the Government has been cracking down on unsolicited calls. In 2007 the Telecom Unsolicited Commercial Communications Regulations, 2007 were issued. Among other things, the regulations established a National Do Not Call Register and a Private Do Not Call List.clvi According to data released by TRAI in 2007, 6.7 million subscribers were registered with the 'Do Not Call' Registry, yet 3,685 of the subscribers still received unsolicited calls.clvii Since the passing of the 2007 Regulations, new Regulations were passed in 2010 known as the "Telecom Commercial Communications Customer Preference Regulations, 2010" (CCCP Regulations).clviii Between 2010 and 2011 eight subsequent amendments were passed.clix The CCCP Regulations work to regulate 'unsolicited commercial communications', which have been defined as any message which is transmitted for the purpose of informing, soliciting, or promoting any commercial transaction in relation to goods, investments or services etc. Excluded from this definition are 'transactional messages', which relate to:

- Information pertaining to the account of a customer and sent by a licensee, bank, insurance company, credit card company, or depositories registered with Securities and Exchange Board of India, or Direct to Home Operators
- Any information given by Airlines or Indian Railways or its authorized agencies to its passengers regarding travel schedules, ticket booking, and reservation,
- Information from a registered educational institution to parents or guardians of its students,
- Any other message as may be specified by the Authority from time to time as a "transactional message".clx

To facilitate regulation of unsolicited commercial communications, the 2007 guidelines established a 'National Do Call Register', and a 'Private Do Not Call List', which are applicable under the CCCP Regulations as well. In addition to the "National Do Not Call Register" and the "Private Do Not Call List", the CCCP Regulations establish the following facilities and categories:

- 'Provider Customer Preference Registration Facility'
- 'Fully blocked' and 'partially blocked' categories
- 'National Customer Preference Register'
- 'National Telemarketers Register'
- 'Provider Customer Preference Register'.

Features of the CCCP Regulations that relate to the privacy principles include:

Oversight

- The TRAI has the right to constitute an inquiry committee to look into the contravention of the CCCP Regulations.[clxi]

Accountability

- It will be the responsibility of the service provider to ensure that no telecom resource is provided to a telemarketer unless it has registered itself with the Authority. The Service Provider must also ensure that the telemarketer scrubs the telephone number of the subscriber with the database received from the NCPR before sending any SMS to a telecom subscriber. Every Service Provider must ensure that commercial communications including SMSs are sent to the customer only between 9am and 9pm.[clxii] However even these measures were not enough to curb the menace of unsolicited marketing calls since most people were using unregistered telemarketers to get around the regulatory framework. Therefore amendments were made to the Regulations in August 2013 which make even the service provider liable for unsolicited calls even if the calls have been made by an unregistered telemarketers.[clxiii] The Regulations further require the service provider to investigate complaints of unsolicited marketing calls and if they find that a call has originated from an unregistered number then the service provider has to disconnect all telecom resources allotted to the number.[clxiv]

Security

- All service providers must put in place appropriate mechanisms to protect the privacy of communications and subscriber information.[clxv]

Access and Correction

- Subscribers have the option to change their preference after three months of initial registration in the NPCPR.clxvi

Purpose Limitation

- **SMS Limit and charge:** The number of permitted SMS's to be sent per day per SIM is a contested issue, and has not been decided yet. In the past, SMS's had been limited to both 100 and 200 SMS's per day. Currently the regulations provide for a limit of 100 SMS's per day on a concessional scheme and anything above that to be charged at a minimum of 50 paise per SMS.

Choice and Consent

- **Provider Customer Preference Register (PCPR):** Every service provider or agency will set up a toll free Customer Preference Registration Facility that will be identified by the code 1909 and will contain a list of subscribers preferring to be fully blocked and partially blocked. The PCPR must include: the name of each subscriber making the request, the telephone and area code of each subscriber, the date and time of making the request, and details of the option chosen by the subscriber, and the unique registration number.clxvii A duplicate copy of the PCPR list will be maintained in at least two places for security purposes. clxviii The Private Do Not Call List, as established under the 2007 regulations will be included in this register.clxix

- **National Customer Preference Register (NPCPR):** The NCPR will be maintained by any agency authorized by the Authority.clxx The Register will contain the telephone number and area code of the subscriber indicating their preference, the details of the preference, and any other information specified by the Authority.clxxi The NCPR should be updated every 24 hours.clxxii

- **National Telemarketer Register:** A National Telemarketer Register shall be set up and maintained by an agency authorized by the Authority. The Register should contain a) details of the telemarketers like registration date, application number, and registration number b) details of the fees deposited by the telemarketer, c) details of the telecom resources allotted to a telemarketer d) the number of notices, along with the date of such notices, served upon the telemarketer by the Access Providers for sending unsolicited commercial communications e) the date of blacklisting of the telemarketer f) other details specified by the Authority. clxxiii For registration, a fee must be paid by the telemarketer, and resources will not be given to the Telemarketer unless it is registered. What resources will be given to the telemarketer is not made clear. Every Telemarketer, after registration, will be identified by the numbers '140' and '70'.clxxiv Telemarketers will be black listed if they fail to furnish additional security information, or if they have received and failed to comply with six notices for sending unsolicited commercial communications.clxxv

Quality/Verification

- After receiving a request to be placed in the NCPR register from a subscriber, the Service Provider must verify the communication and send a unique registration number to the subscriber within 24 hrs.clxxvi

Penalty/Offenses/Liability/Remedy

- Complaint mechanism: If an individual still receives unsolicited commercial communications 7 days after registering in the PCPR, he/she may issue a complaint using the code 1909. While making the complaint, the subscriber must provide the particulars of the telemarketer, the telephone number of the unsolicited commercial communications, the date & time, and a brief description of the unsolicited commercial communication. The Terminating Access Provider must acknowledge the complaint with a unique complaint number, and within seventy two hours forward the

complaint to the National Telemarketer Register and to the Originating Access Provider from whose network such unsolicited commercial communications originated and take needed action. [clxxvii]

- Penalty:

Offence	Fine
If an inquiry is conducted and the service provider is found to have contravened the provisions.	One lakh rupees and in the case of the second contravention five lakh rupees and on the third and each subsequent contravention ten lakh rupees. [clxxviii]

Missing Principles

- Notice
- Collection Limitation
- Disclosure
- Openness

Case Law: TRAI Guidelines

Despite having in place guidelines for the regulation of Unsolicited Commercial Communications, implementation has been a challenge. For example, beginning in 2006 and lasting through 2010, a Supreme Court division bench issued a notice against Cellular Operators Association of India, Bharati Airtel, ICICI Bank, and American Express Bank seeking explanation from them as to whether they should be penalized for unsolicited calls/messages on a petition filed by Nivedita Sharma. The State Consumer Commission (Delhi), imposed a fine amounting to Rs 50 lakh on telecom companies and Rs 25 lakh on private banks along with Rs 50,000 to Sharma on account of mental harassment suffered by her. However, the costs were set aside by Delhi High Court. Thus, the State Consumer Commission ordered TRAI to put in place a 'do not call' register and bring in a number portability rule.[clxxix] Later, in contravention to the fine imposed by State Consumer Commission and the TRAI policy, ICICI bank failed to pay the fine to Nivedita Sharma, whereupon a contempt proceeding was filed before the commission by her. On an application preferred by ICICI to the Delhi High Court bench, the High Court refused to stay the contempt proceedings and said, "You think you are above the law? Every day we receive calls at all times of the day from ICICI for loans, credit cards...now you face the music"[clxxx]

For example, in 2006 the issue of telemarketing practices was brought before the courts as a Public Interest Litigation. The case argued that indiscriminate calls made by companies constituted an invasion of privacy. During the hearing, the bench was clear about the need to

regulate and curtail telemarketers' unlimited and free access to mobile numbers. Out of the hearing came the first suggestions for a 'do not disturb' register in India, and the assignment of a prefixed number for telemarketers, enabling easy identification.[clxxxi] In

Problem is all we know about this case is from news reports, I tried to access the orders in this case but I could only get hold of one order (there have been many orders issued in this case) and that one also wasn't very helpful, it was only half a page. Its probably best not to mention it specially since it's an old case.

Projects and Practices

.IN Registration

An individuals ability to use the Internet anonymously is also limited by the .IN requirements for registration of a domain name. Unlike many countries, .IN, which is regulated by the National Internet Exchange, does not allow for anonymous registration. For example, the Terms and Conditions for Registrants require registering individuals to provide contact details including their full name, postal address, email address, voice & telephone number, and fax number. Registering individuals are also not allowed use proxy services, and are held liable for breaches of the terms and conditions.[21]

Phishing, Hacking, and Fraud

According to statistics, India is among the top three countries which is a target of phishing attacks. Commonly, the targets are various banks and government organizations such as the Income Tax Department. It was reported by CERT-In that there were 3 cases of phishing in the year 2004, and 392 cases of phishing in 2007.[clxxxii] According to additional government data, there were 386 phishing incidents reported to the CERT-In between January and October, 2011.[clxxxiii]

One of the first cases of phishing was registered with the Cyber Crime Investigation Cell in the year 2005 by a financial institute. It was alleged that the accused was involved in sending e-mails which appeared to be sent by ICICI Bank. The e-mail requested personal and confidential information from clients. Out of 120 customers that were targeted with the fraudulent email, 80 divulged their banking details, under the impression that it was a genuine request. The accused was charged under Section 66 of the ITA and Sections 419, 420, 465, 468, 471 of the IPC read with Section 51, 63 and 65 of the Copyright Act, 1957[clxxxiv] Similarly, in 2007, the website of Bank of India was hacked and malware was planted on the site. The malware installs itself on the computers of the visitors and sends sensitive information to the hacker. In another case, a Malaysian national hosted a website which was a replica of the Axis Bank website, duping the customers to part with their confidential passwords and other details.clxxxv

In 2008, Mr Gulshan Rai, Director General in the Union Ministry of Communication and Information Technology said that the Government has made an effort to define spam and phishing and online frauds. However, it was not defined by the Information Technology

[21] Terms and Conditions for Registrants. Point 1 and 3. Available at: http://www.registry.in/system/files/Terms_and_Conditions_for_Registrants_1.pdf. Last Accessed: August 6th 2012.

(Amendment) Act, 2008. Mr. Rai also noted that, "[t]he number of phishing cases is also increasing among the Indian banks. Almost 7-8 cases of phishing are being reported on an average daily and most of them are hosted from outside … hosted in one country, registered in another country".clxxxvi

The problem of phishing is widely recognized by banks in India, though it appears as though they do not like to take responsibility for phishing attacks. In 2011, a former top official of the India Overseas Bank conceded that "most of the time banks pass the responsibility of recovering the money to the customers. They also avoid accepting the incidence of such cases as it may result to damage to its reputation and good will." It was also reported that RBI has laid down certain guidelines banks must follow when they experience fraud, but most of the banks do not follow the guidelines.clxxxvii

In 2012, six foreign nationals were arrested suspected of defrauding people by using text message and email scams. The victims of the scam were told that they have won lottery.clxxxviii "These people have software generating e-mail ids and mobile numbers. They would randomly select them and send thousands of SMSes and e-mails every day," said Joint Commissioner of Police of Mumbai, Himanshu Roy[clxxxix]. Also in 2012 a press statement from the Ministry of Communications & Technology alleged that the website of Bharat Sanchar Nigam Limited had been hacked in 2011, and from December 2011-February 2012 112 Government websites were hacked. The statement also noted that according to the Reserve Bank of India, for the years 2009, 2010, and 2011 5,288 internet frauds took place for amounts ranging between Rs. 1 lakh and above.[cxc]

National E-Governance Plan (NeGP)

In May 2006, the Indian government approved the National E-Governance Plan (NeGP), which was conceptualized as a comprehensive approach towards making government services available to people in their specific localities while meeting goals of efficiency, transparency, reliability, and affordability. Broadly speaking, the infrastructure, governance, and implementation of the National E-Governance plan has many privacy implications. For example, it is proposed to create State Data Centres in order to allow States to consolidate services. The State Data Centre will facilitate services such as: Citizen Information/Services Portal, State Intranet Portal, Disaster Recovery, Remote Management and Service Integration etc. The Department of Information and Technology (DIT) has created guidelines for the Technical and Financial Support for Establishment of State Data Centres[cxci] Among other things, the guidelines envision a data retention plan that would be formulated by the State,[cxcii] mechanisms that ensure physical and network security, and puts inplace security audits for every six months. [cxciii] The DIT has also created a best practices and guidelines document outlining best practices in data security that the State must develop and enforce when running a State Data Center. Broadly, the guidelines place the obligation on the State to develop and implement trust and identity management policies, security posture assessments, data privacy polices, ensure confidentiality and monitor access to data, and implement disaster recovery and business continuity plans.[cxciv]

The NeGP also envisions the development of Common Services Centers (CSC). CSC's are computer resource centers designed to provide an accessible facility for the delivery of e-services in rural and remote areas. Services that will be provided at CSC's include information relating to health, education, agriculture, and employment. Individuals will also be able to complete payments like NREGA, utility payments, and access online banking services. As envisioned, the project has a three tiered governance framework that includes 1.

State Designated Agencies involved in monitoring and supervising the CSC at the state level. 2. A Service Centre Agency – meant to provide the required investment budget and the functional specifications for the CSC 3. Village Level Entrepreneur in charge of running daily operations at the CSC.[cxcv] An example of how CSC's could be used can be see through DITs proposal to leverage the CSC network for the carrying out of the NPR project by capturing and entering data at centers.[cxcvi]

Public Information Infrastructure[cxcvii]

In 2009, Prime Minister M. Singh appointed Sam Pitroda to the cabinet-level position of Adviser to the Prime Minister for Public Information Infrastructure[cxcviii] and Innovations, tasked with developing a unified policy for information standards and practices incorporating both intra-government affairs and citizens' services. In June 2010, Mr. Pitroda's office uploaded an online a slide presentation on "Strengthening Democracy and Governance: Public Information Infrastructure." The presentation provides a basic overview of his proposal for a robust information system. Included in the scheme is the development of a national repository of information on people, including citizenship, resident, and household data; places, including villages, towns, streets, schools, hospitals, government offices, factories, officers, residences, stations, mines, minerals, dams, plants, rivers, parks, forests, farms, etc.; and programs and other government offices, such as the National Rural Employment Guarantee Scheme, the Public Distribution System, girl child benefit schemes, pensions, the judiciary, police and prisons, treasuries, land records, universalize elementary education, and the National Rural Health mission, among others. Applications hosted on the PII will include a shared Geographic Information System (GIS) for the Survey of India; the National Disaster Management program; the Urban Ministry; the Departments of Space, Security, Environment, Health, and Rural Development; the Planning Commission; as well as private enterprises. Data from these entities will be publicly available on a single portal accessible by a variety of clients, including PCs and mobile phones. The portal will also incorporate applications, communities, mash-ups, and allow for a variety of analyses on data including including survey, remote sensing data, census, education, and health data, as well as forest, land use and groundwater data.[cxcix]

National Data Sharing and Accessibility Policy

This policy[cc] was approved by the Union Cabinet on February 9th 2012. The policy is a broad framework that applies to all data and information created, generated, collected and archived using public funds provided by the Government of India for the purposes of enabling *ready access to valuable data is essential for a number of decisions and tasks including development planning, controlling disasters, and national security.* The policy focuses on integrating all governmental databases to facilitate governmental access to information, and is based off of principles like: Openness, Flexibility, Transparency, Legal Conformity, Protection of Intellectual Property, Formal Responsibility, Professionalism, Standards, Interoperability, Quality, Security, Efficiency, Accountability, Sustainability, and Privacy. A data warehouse will be set up to house current and historical data so that this information in is one place.

The policy divides types of data between shareable data and non shareable data, and creates multiple levels of access to data including: open access, registered access, and restricted access. It is also envisioned that all departments will prepare a list of data that is not to be

shared within six months of notification. All other data sets will be considered safe to be opened to the public. Meta Data would also be provided which would allow people to know what data is available Different steps for implementation of the scheme have been outlined such as making data available on an "as-is where-is' basis, and requiring that all valuable data sets be uploaded by the end of three months, all data sets be uploaded by the end of this year, and after that – be updated on a quarterly basis etc. Privacy concerns associated with the policy include possibility of function creep and misuse of data from the integration and sharing of data across governmental departments. Furthermore, the lack of clarity over which authority will be responsible for allowing or restricting access to data creates a vulnerability in the security of the policy.

National Knowledge Commission recommendations

In June 2005, Prime Minister M. Singh constituted the National Knowledge Commission (NKC), an advisory body to the Office of the Prime Minister, with the mandate to recommend[cci] policy reforms in the areas of "access to knowledge, creation and preservation of knowledge systems, and dissemination of knowledge and better knowledge services." After three years of review, the NKC issued a series of reports in the "National Knowledge Commission Final Report 2006-2009." In its Final Report, the NKC made two recommendations particularly relevant to implementing open government data in India. First, the NKC "recommended the establishment of a high-end National Knowledge Network connecting all … knowledge institutions in various fields and at various locations throughout the country, through an electronic digital broadband network with gigabit capacity". Second, the NKC proposed that the government create a series of "national web based portals on certain key sectors such as Water, Energy, Environment, Teachers, Biodiversity, Health, Agriculture, Employment, Citizens Rights etc. that would serve as a single window for information on the given sector for all stakeholders" . The NKC also recommended that government departments should make data sets they have available in a digital format. It is unclear to what extent this recommendation has been followed.

Private Public Partnerships

As governments move towards implementing e-governance projects, they engage with private entities through Public Private Partnerships (PPPs) to help in the design, implementation, and delivery of services. Though these businesses help in designing and implementing various projects, privacy becomes a concern when the private sector collects personal information, as often the information is protected only through contract. An example of how PPP's challenge privacy can be seen through the project developed between Tata Consultancy and the Indian Government. In October 2008, Tata Consultancy Services a prominent software services company in India was awarded a Rupees 1000 crore project to "provide passport-related services to Indian citizens in a speedy, convenient and transparent manner."[ccii] In the absence of anything in the Passport Act prohibiting the outsourcing of essential functions, the task of safeguarding of citizens' privacy falls to the domain of contract law – assuming the contract between the state and the company contained a standard confidentiality clause - and the limited provisions of the IT Act dealing with data protection. The contractual option does not provide reliable privacy safeguard since it is only enforceable by the state against the private company and the state has had, at best, a patchy record has of defending its contractual rights against private companies. The following extract, from a newspaper account about the outsourcing of biometric data collection illustrates the fluidity with which data sharing across databases occurs today between governments and contracted companies.*"The project, conceived by WFP in 2007, was started a year ago with Hyderabad-*

based 4G Identity Solutions Pvt. Ltd as technology partner. Using its 125-member team, the firm digitized old ration card registers and mapped these with the database of the 1997 BPL survey and 2002 household survey. The gram panchayat target beneficiary database was then transferred to some 6,000 enrollment stations in 2,445 villages, 41 wards and three urban local bodies where people queued up to get their biographic and biometric data recorded. Data from enrollment stations were sent to the 4G data centre for aggregation where de-duplication was done using a multi-modal biometric engine to check for fake enrollments. A final database of unique card holders was generated and stored in a centralized citizen database. Rural households have been given laminated bar-coded ration cards and coupons since point-of-sale machines cannot be used in villages, several still without electricity." Indian Express, August 2003[cciii]. Though PPP's can greatly help in the delivery and development of infrastructure and services, it is important that the project is regulated by more than just a contract in order to protect the privacy of the data.[cciv]

State wide E-Governance infrastructure

Increasingly, various states have taken initiatives to transform entire government services and infrastructure to be digital. For instance, in 2012 the State of Kerala announced that it would soon making the state 'fully digital'. This will include providing every citizen with an e-mail ID that would be based on their UID number, thus allowing all communications, transactions, and applications between the government and the citizen would take place through e-mail. Pensions and scholarships would be distributed to entitled individuals via the banks, and all government files will be converted to the digital mode.ccv The underlying architecture to these plans include the establishment of a department wide network which will connect governmental departments and public offices. This network will allow all connected departments to access data, voice, and video services. The department wide network will then be connected to the Kerala State Wide Area Network.ccvi Questions related to privacy that the initiative raises include: how will the State ensure that citizens email connections are secure and not accessible by different government departments, how will the state ensure accuracy in converting documents to the digital form, and what security measures will be put in place to ensure that as governmental databases are created – unauthorized access, collation, data mining, and tracking do not take place.

MCA21

In 2006 the Ministry of Corporate Affairs (MCA), Government of India, began to put in place plans for a project known as MCA21. [ccvii] In 2012, the Government has pushed to finish the project. The project aims to convert processes, transactions, and legal requirements found under the Companies Act to the digital. The objective of the service is to allow for transparency and tracking of corporate activities in order to identify and resolve suspicious and fraudulent corporate transactions.[ccviii] Components of the project that impact privacy and that are still unclear include: the extent of information that will be collected, how this information will be stored/secured/deleted, and who will have access to the information.

TAGUP[ccix]

In February 2011 the Unique Identification Authority of India (UIDAI) Chairman, Nandan Nilekani, submitted a seven-member group's report detailing specific recommendations for IT-intensive projects such as the Tax Information Network (TIN), New Pension Scheme (NPS), National Treasury Management Agency (NTMA), Expenditure Information Network (EIN) and Goods and Service Tax (GST). Among the recommendations, the TAGUP has envisioned that to handle all aspects of IT systems for governmental projects, a National

Information Utilities (NIU) will be put in place. The report calls for the use of open data, open standards, using open source, and envisions an interoperable system. Among other things, the report recommends that designers of e-gov projects should take pro-active actions in deciding what information to share publicly, as most information held by the government is required to be shared under the RTI Act. The report also broadly recognizes the need to protect the privacy of data entered into the system and recommends guidelines that could be included in a privacy legislation. The recommended guidelines include the following:

- *Solution architecture and privacy*: A privacy legislation should put in place rules that can be implemented and incorporated into IT systems and projects from the very start of the project.[ccx]
- *Personal Identifiable Information*: Personal Identifiable information should be stored separate from other data and in an encrypted form. Separate access controls should be defined for personal identifiable information, and unauthorized access should be penalized. [ccxi]
- *Anonymization of Data:* Data should be anonymized when released to the public. The method of anonymization should follow the logic of k-anonymity – where each record is indistinguishable from k-1 other records.[ccxii]
- *Data Retention:* Data retention policies should be well defined. If records are needed to be retained for long periods of time, personal identifiable information should be scrubbed from logs after a pre-defined time. Individuals should be able to access personal data stored in the IT system after authenticating their identity.[ccxiii]
- *Balancing the Right to Privacy with Public Interest:* In the case of national security, economic offenses, tax evasion, and other specified circumstances, Government agencies will need to access or share data. This access should be permitted, but should be carefully regulated by a data protection regime.

Bhoomi

Bhoomi[ccxiv] is an e-governance initiative that works to computerize land records. The project was started in Karnataka and designed by the National Informatics Centre (NIC). It focuses on enhancing the delivery and management of land records. The objective of BHOOMI is to reduce the discretion of public officials by allowing for individuals to issue a mutation request online. This allows any individual (farmer & non farmers) to access the database. Individuals who apply online can obtain a printed copy of the RTC by providing the name of the owner or plot number at computerized land record kiosks in taluk offices. A second computer screen faces the clients to enable them to see the transaction being performed. A farmer can check the status of a mutation application on Touch Screen Kiosks. If the revenue inspector does not complete the mutation within 45 days, an individual can approach a senior officer with their grievance.

Important features of the project related to privacy:

- *Security***:** The Bio-logon metrics authenticates various users on the Bhoomi software on the basis of fingerprints. This measure ensures that no one can hack into the system by imitating other users.
- *Authenticity***:** Original mutation orders of the revenue inspector (who is the authorized person to pass orders in the mutations in the field) and notices served on interested parties are scanned to ensure authenticity and accuracy.

- *Access:* The Bhoomi system is open to all individuals who have a 'revenue number.' The implication of this is that persons who are not the owners of the land are able to collect RTC papers from a Bhoomi Kiosk by quoting a 'revenue no.' Though access is important to facilitate the transparency that the system hopes to achieve, it is possible for this information to be misused.
- *Transparency:* The system makes all division, buying, and selling of land transparent to the public. This gives individuals the ability to follow the transactions of bureaucrats and public officials and monitor the amount of their accumulated wealth. On the other hand, because of the transparency of the system privacy infringing circumstances can come about. For example, Banks who are performing 'due diligence' checks have the ability to access client land records without obtaining prior consent.

Interception

In India, reports of state-sponsored surveillance did not begin to emerge until the 1970s, during Prime Minister Indira Gandhi's declared 'State of Emergency'. The state-sponsored wiretapping that took place during the Emergency changed the nature and justification of surveillance in India from monitoring foreign countries and actors so as to protect citizens and the Government, to monitoring citizens to protect citizens and the Government. This change in the justification for surveillance has influenced subsequent Indian legislation and foreign intelligence policies. India has had a long history of conflicts - from the Kashmir conflict (1962), to the Indo-Pakistani war (1971), to the Kargil war (1999), to the multiple terror attacks throughout the country. In conformance with global surveillance trends, the Indian Government too has responded to these conflicts and acts of violence by reforming local and state law and enforcement, through the creation of niche intelligence agencies, and through a steady expansion of intelligence powers at the Central and State levels. In democracies, because of the freedom of speech that wiretapping seemingly threatens, governments and civil society are usually in constant renegotiation over the details of the wiretapping regime. These negotiations are usually precipitated by the introduction of a new generation of telecommunication technology or laws enacted which conflict with personal liberties. For instance, in India during the 1980's, the People's Union for Civil Liberties (PUCL) staged protests asking for the repeal of certain clauses in Indian interception law.[22]

That said, the Indian Government has a long history of conducting authorized and unauthorized interceptions of communications. For example, during the 'Sikh Terrorism' in 1986, the Government declared nearly half of Punjab as "disturbed" zone. Because of this declaration, the police, under the Terrorist and Disruptive Activities (Prevention) Act, 1987 had the power to open private mails, tap telephones, listen into conversations, and take control of telephones on subjective satisfaction that the said telephone is being used to aid terrorism/communication with people assisting terrorists. The Act empowered the police to take measures without prior approval.[ccxv] With the development of technology, the Government has passed laws which legitimize the interception of all forms of communication including e-mails, sms's, mobile phone calls, instant messaging, etc.

22 http://www.pucl.org/from-archives/Media/mail-phone.htm

[i] BBC. India Facebook arrests: Supreme Court demands explanation. BBC. November 30th 2012. Available at: http://www.bbc.co.uk/news/world-asia-india-20551955. Last Accessed February 18th 2013.

[ii] *R. Rajagopal* v. *State Of T.N*, http://indiankanoon.org/doc/501107/; and summarized in *Naz Foundation* v. *Government of Delhi*,W.P. (C) No. 7455/2001, (2009) http://www.nazindia.org/judgement_377.pdf

[iii] ITA 2008 section 75

[iv] ITA 2008 66E

[v] The Criminal Law (Amendment) Ordinance, 2013. Section 354C. Availabe at: http://haryanapolice.gov.in/The_Criminal_Law_Amendmen_-Ordinance_2013_Promulgated_on_3rd_Feb_2013.pdf

[vi] This analysis was pointed out by NAAVI in the post Women's protection Ordinance Clashes with ITA 2008. February 2013. Available at: http://www.naavi.org/wp/?p=744

[vii] Ministry of Home Affairs. January 4th 2012. Advisory on Preventing & Combatting Cyber Crime against Children. Available at: http://www.mha.nic.in/pdfs/CS-Adv-160112.pdf

[viii] ITA section 72

[ix] Section 84A of the Information Technology Act, 2000 (as amended by the Information Technology (Amendment) Act, 2008).

[x] ISP license section 2.2(vii)

[xi] . Information Technology (Electronic Service Delivery) Rules, http://bit.ly/Q5OsZr

[xii] Information Technology (Guidelines for Cyber Cafe) Rules, 2011, Rule 5(3)

[xiii] Information Technology (Guidelines for Cyber Cafe) Rules, 2011, Rule 7(1)

[xiv] Software Freedom Law Center. (2012). *Look Who's Watching.* March 5th . Accessed March 28th. Available at: http://softwarefreedom.in/index.php?option=com_idoblog&task=viewpost&id=126&Itemid=70

[xv] Information Technology Act, 2000 s. 28

[xvi] Information Technology Act, 2000 s. 29

[xvii] IT Interception Rules, 2009, Rule 2(d)**:** 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.

[xviii] IT Interception Rules, 2009, Rule 3

[xix] Information Technology Act, 2000, s. 69(1)

[xx] Information Technology Act, 2000, s. 69(1)

[xxi] IT Interception Rules, 2009, Rule 4

[xxii] IT Interception Rules, 2009, Rule 5

[xxiii] ITA Interception Rules, 2009, Rule 22

[xxiv] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, Rule 7

[xxv] ITA Interception Rules, 2009, Rule 12

[xxvi] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, Rule 18

[xxvii] IT Interception Rules, 2009, Rule 3.

[xxviii] IT Interception Rules, 2009, Rules 7 and 10

[xxix] IT Interception Rules, 2009, Rule 7

[xxx] IT Interception Rules, 2009, Rule 8

[xxxi] IT Interception Rules, 2009, Rule 11

[xxxii] IT Interception Rules, 2009, Rule 3.

[xxxiii] IT Interception Rules, 2009, Rule 6.
[xxxiv] IT Interception Rules, 2009, Rule 13(1).
[xxxv] IT Interception Rules, 2009, Rule 19
[xxxvi] IT Interception Rules, 2009, Rule 17
[xxxvii] Information Technology Act, 2000, s.69 (2)
[xxxviii] Information Technology (Intermediary Guidelines) Rules, 2011, Rule 3(1)
[xxxix] Information Technology (Intermediary Guidelines) Rules, 2011, Rule 3 (5)
[xl] Information Technology (Intermediary Guidelines) Rules, 2011, Rule 3 (7)
[xli] Information Technology (Guidelines for Cyber Cafe) Rules, 2011, Rule 6(6)
[xlii] Information Technology (Guidelines for Cyber Cafe) Rules, 2011, Rule 6 (5)
[xliii] Information Technology (Guidelines for Cyber Cafe) Rules, 2011, Rule 6(1)&(2)
[xliv]. Information Technology (Electronic Service Delivery) Rules, 2011, Rule 3(3).
[xlv]. Information Technology (Electronic Service Delivery) Rules, 2011, Rule 5 (4).
[xlvi] ITA Interception Rules, 2009, Rule 20& 21
[xlvii] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, Rule 20
[xlviii] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, Rule 25
[xlix]. Information Technology (Electronic Service Delivery) Rules, 2011, Rule 8(4).
[l] Information Technology (Intermediary Guidelines) Rules, 2011, Rule 3 (7)
[li]. Information Technology (Electronic Service Delivery) Rules, 2011, Rule 8(3).
[lii] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, Rule 25(2)&(6)
[liii] Information Technology (Intermediary Guidelines) Rules, 2011, Rule 3(2) (a-i)
[liv] Information Technology (Intermediary Guidelines) Rules, 2011, Rule 3 (4)
[lv] Information Technology Interception Rules, 2009, Rule.4
[lvi] Information Technology Act, 2000, s.69(1)
[lvii] Information Technology Act, 2000, s.69(1)
[lviii] Information Technology Act, 2000, s.69 (1)
[lix] Information Technology Act, 2000, Section 69B
[lx] Information Technology (Intermediary Guidelines) Rules, 2011, Rule 3 (4)
[lxi] Information Technology (Guidelines for Cyber Cafe) Rules, 2011 Rule 4(2)
[lxii] Information Technology (Guidelines for Cyber Cafe) Rules, 2011, Rule 5(1)
[lxiii] Information Technology (Guidelines for Cyber Cafe) Rules, 2011, Rule 5(2)
[lxiv] Information Technology (Guidelines for Cyber Cafe) Rules, 2011, Rule 5(3)
[lxv] Information Technology (Guidelines for Cyber Cafe) Rules, 2011, Rule 5(4)
[lxvi] Information Technology (Guidelines for Cyber Cafe) Rules, 2011Rule 4(1)-(4)
[lxvii]. Information Technology (Electronic Service Delivery) Rules, 2011, Rule 5(1)(2).
[lxviii]. Information Technology (Electronic Service Delivery) Rules, 2011, Rule 7.
[lxix] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, Rule 23
[lxx] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, Rule 23(2)
[lxxi] Information Technology (Intermediary Guidelines) Rules, 2011, Section 3(5)
[lxxii]. Information Technology (Electronic Service Delivery) Rules, 2011, Rule 6(2).
[lxxiii] Information Technology (Intermediary Guidelines) Rules, 2011, Rule 3 (11)
[lxxiv] Information Technology Act, 2000, s. 43
[lxxv] Information Technology Act, 2000 (as amended by the Information Technology (Amendment) Act, 2008) s. 66F

[lxxvi] Information Technology Act, 2000 (as amended by the Information Technology (Amendment) Act, 2008) s. 66E.

[lxxvii] Information Technology Act, 2000 (as amended by the Information Technology (Amendment) Act, 2008) s. 67B (a-e)

[lxxviii] ITA 2008 section 72

[lxxix] ITA 2008 section 72A

[lxxx] Information Technology Act, 2000, (as amended by the Information Technology (Amendment) Act, 2008), s. 69A(3)

[lxxxi] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, Rule 24 (1) read with Section 72 of Information Technology Act, 2000

[lxxxii] Available at http://delhihighcourt.nic.in/dhcqrydisp_O.asp?pn=163416&yr=2013

[lxxxiii] Available at http://delhihighcourt.nic.in/dhcqrydisp_O.asp?pn=163416&yr=2013

[lxxxiv] Indian Telegraph Act, 1951, s.5(2)

[lxxxv] Rule 419A(1) of the Indian Telegraph Rules, 1951, as inserted by Section 2 of Interception Rules, 2007

[lxxxvi] Rule 419A(1) of the Indian Telegraph Rules, 1951, as inserted by Section 2 of Interception Rules, 2007

[lxxxvii] Section 419A(1) of the Indian Telegraph, 1951, as inserted by Section 2 of Interception Rules, 2007

[lxxxviii] Rule 419A(16) of the Indian Telegraph Rules, 1951, as inserted by Section 2 of the Interception Rules, 2007

[lxxxix] Rule 419A(9) of the Indian Telegraph Rules, 1951, as inserted by Section 2 of the Interception Rules, 2007

[xc] Rule 419A(2) of the Indian Telegraph Rules, 1951, as inserted by Section 2 of the 2007 Interception Rules, 2007

[xci] Rule 419A(7) of the Indian Telegraph Rules, 1951, as inserted by Section 2 of the Interception Rules, 2007

[xcii] Rule 419A(10) of the Indian Telegraph Rules, 1951, as inserted by Section 2 of the Interception Rules, 2007

[xciii] Rule 419A(8) of the Indian Telegraph Rules, 1951, as inserted by Section 2 of the Interception Rules, 2007

[xciv] Rule 419A(11) of the Indian Telegraph Rules, 1951, as inserted by Section 2 of the Interception Rules, 2007

[xcv] Rule 419A(13) of the Indian Telegraph Rules, 1951, as inserted by Section 2 of the Interception Rules, 2007

[xcvi] Rule 419A(14) of the Indian Telegraph Rules, 1951, as inserted by Section 2 of the Interception Rules, 2007

[xcvii] Rule 419A(14) of the Indian Telegraph Rules, 1951, as inserted by Section 2 of the Interception Rules, 2007

[xcviii] Rule 419A(5) of the Indian Telegraph Rules, 1951, as inserted by Section 2 of the Interception Rules, 2007

[xcix] Indian Telegraph Act, 1951, s.5(2)

[c] Rule 419A(2) of the Indian Telegraph Rules, 1951, as inserted by Section 2 of the Interception Rules, 2007

[ci] Rule 419A(4) of the Indian Telegraph Rules, 1951, as inserted by Section 2 of the Interception Rules, 2007

[cii] Rule 419A(6) of the Indian Telegraph Rules, 1951, as inserted by Section 2 of the 2007 Interception Rules, 2007

[ciii] Rule 419A(3) of the Indian Telegraph Rules, 1951, as inserted by Section 2 of the Interception Rules, 2007
[civ] Rule 419A(18) of the Indian Telegraph Rules, 1951, as inserted by Section 2 of the Interception Rules, 2007
[cv] Rule 419A(19) of the Indian Telegraph Rules, 1951, as inserted by Section 2 of the Interception Rules, 2007
[cvi] Rule 419A(17) of the Indian Telegraph Rules, 1951, as inserted by Section 2 of the Interception Rules, 2007
[cvii] Rule 419A(15) of the Indian Telegraph Rules, 1951, as inserted by Section 2 of the Interception Rules, 2007
[cviii] Indian Telegraph Act, 1951, s. 25
[cix] http://indiankanoon.org/doc/1769219/.
[cx] ITA Interception Rules, 2009, Rule 4
[cxi] Rule 419A of the Indian Telegraph Rules, 1951, as inserted by Section 2 of the Interception Rules, 2007
[cxii] ITA Interception Rules, 2009, Rule 4
[cxiii] Rule 419A(15) of the Indian Telegraph Rules, 1951, as inserted by Section 2 of the Interception Rules, 2007
[cxiv] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, Rule 13 (2) &(3)
[cxv] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, Rule 17
[cxvi] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, Rule 19
[cxvii] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, Rule 23(2)
[cxviii] Rule 419A(19) of the Indian Telegraph Rules, 1951, as inserted by Section 2 of the Interception Rules, 2007
[cxix] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, Rule 24
[cxx] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, Rule 25(6)
[cxxi] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, Rule 6
[cxxii] ISP License, s.34.28 (xix)
[cxxiii] ISP License, s.30.1
[cxxiv] ISP License, s. 34.12
[cxxv] ISP License, s. 34.13
[cxxvi] ISP License, s.34.22
[cxxvii] ISP License, 34.6
[cxxviii] ISP License, 34.15
[cxxix] ISP License, s.34.17
[cxxx] ISP License, s.34.11
[cxxxi] ISP License, 34.28 (xiv)
[cxxxii] ISP License, s.34.28 (xi)
[cxxxiii] ISP License, s.34.14
[cxxxiv] ISP License, s.34.24
[cxxxv] ISP License, s.34.28 (ix)&(x)
[cxxxvi] ISP License, s. 30.1

[cxxxvii] ISP License, s. 33.4
[cxxxviii] ISP License, s.34.1
[cxxxix] ISP License, s. 34.4
[cxl] ISP License, s.34.7
[cxli] ISP License, s.34.9
[cxlii] ISP License, s.34.27 (a)(i)
[cxliii] ISP License, s.34.27(a)(ii-vi)
[cxliv] ISP License, s. 34.8
[cxlv] ISP License, s. 32.1, 32.2 (i)(ii), 32.3
[cxlvi] ISP License, s. 34.8
[cxlvii] ISP License, s.34.18
[cxlviii] ISP License, s.34.23
[cxlix] ISP License, s.34.28 (xv)
[cl] UASL License, s.41.10
[cli] UASL License, s.41.10
[clii] UASL License, s.41.19(i)
[cliii] UASL License, s.41.19(ii)
[cliv] UASL License, s.41.19(iv)
[clv] UASL License, s. 41.14
[clvi] Dhananjay Mahapatra, Telemarketers to pay fine for first violation, The Times of India, July 28, 2007, available at http://articles.timesofindia.indiatimes.com/2007-07-28/india/27988079_1_telemarketers-violation-harsh-pathak (last visited on Jan. 27, 2012)
[clvii] 3865 subscribers receive unsolicited calls, The Financial Express, Nov. 27, 2007, available at http://www.financialexpress.com/news/3-685-subsribers-receive-unsolicited-calls/244240/0 (last visited on Jan. 27, 2012)
[clviii] The Telecom Commercial Communications Customer Preference Regulations, 2010. Available at: http://210.212.198.149:8080/jspui
[clix] For list of amendments see: http://www.nccptrai.gov.in/nccpregistry/AmendmentToRegulations.jsp
[clx] The Telecom Unsolicited Commercial Communications Regulations, 2010, Regulation 2 (ab)
[clxi] The Telecom Commercial Communications Customer Preference Regulations, 2010, Regulation 21
[clxii] The Telecom Commercial Communications Customer Preference Regulations, 2010, Regulation 20
[clxiii] The Telecom Commercial Communications Customer Preference Regulations, 2010, Regulation 22(1-A)
[clxiv] The Telecom Commercial Communications Customer Preference Regulations, 2010, Regulation 19(11)(a)
[clxv] The Telecom Commercial Communications Customer Preference Regulations, 2010, Regulation 20 read with Schedule IV agreement between access provider and telemarketer
[clxvi] The Telecom Commercial Communications Customer Preference Regulations, 2010, Regulation 8
[clxvii] The Telecom Commercial Communications Customer Preference Regulations, 2010, Regulation 5
[clxviii] The Telecom Unsolicited Commercial Communications Regulations, 2010, Regulation 4(2)
[clxix] The Telecom Unsolicited Commercial Communications Regulations, 2010, Regulation 4(1) Proviso

[clxx] The Telecom Commercial Communications Customer Preference Regulations, 2010, Regulation 6

[clxxi] The Telecom Commercial Communications Customer Preference Regulations, 2010, Regulation 6 (2)

[clxxii] The Telecom Commercial Communications Customer Preference Regulations, 2010, Regulation 10

[clxxiii] The Telecom Commercial Communications Customer Preference Regulations, 2010, Regulation 13(1) (2)

[clxxiv] DoT issued a letter vide No. 16-5/2009-AS.III(Vol.IV) dated 31st January, 2011.

[clxxv] The Telecom Commercial Communications Customer Preference Regulations, 2010, Regulation 18

[clxxvi] The Telecom Commercial Communications Customer Preference Regulations, 2010, Regulation 7 (1) & (2)

[clxxvii] The Telecom Commercial Communications Customer Preference Regulations, 2010, Regulation 19 (1-11)

[clxxviii] The Telecom Commercial Communications Customer Preference Regulations, 2010, Regulation 22

[clxxix] Cell operators get notice on unsolicited phone calls, The Times of India, Aug 27, 2010 available at http://articles.timesofindia.indiatimes.com/2010-08-27/india/28291283_1_nivedita-sharma-unsolicited-commercial-communications-unsolicited-telemarketing (last visited on Jan. 27, 2012)

[clxxx] Abhinav Garg, HC to ICICI Bank: Face the music for making unsolicited calls for making unsolicited calls, The Times of India, Oct. 22, 2008, available at http://articles.timesofindia.indiatimes.com/2008-10-22/mumbai/27935245_1_nivedita-sharma-contempt-proceedings-icici-bank (last visited on Jan. 27, 2012)

[clxxxi] Stop unsolicited calls on cell phones: SC, The Times of India Mar. 7, 2006 available at http://articles.timesofindia.indiatimes.com/2006-03-07/india/27815215_1_harsh-pathak-mobile-phone-users-cellphones (last visited on Jan. 27, 2012)

[clxxxii] Mayank Tewari, India phishing in troubled waters, DNA, Apr. 8, 2008, available at http://www.dnaindia.com/india/report_india-phishing-in-troubled-waters_1158977 (last visited on 25/01/2012)

[clxxxiii] Shanthi Kannan, Safeguard passwords from phishing attacks,The Hindu, Jan. 22, 2012 available at http://www.thehindu.com/sci-tech/internet/article2823567.ece (last visited on 25/01/2012)

[clxxxiv] Cyber Crime Cell, Mumbai: Case of Phishing. Mumbai Police. available at: http://cybercellmumbai.gov.in/html/case-studies/case-of-fishing.html (last visited on Jan. 23, 20120

[clxxxv] Aniruddha Ghosh, Banks are new targets for hackers, The Economic Times, Sept 12, 2007, available at http://articles.economictimes.indiatimes.com/2007-09-12/news/28406155_1_phishing-indian-banks-hacker

[clxxxvi] Amended IT Bill likely to get nod this session, The Hindu Business Line, Dec. 5, 2008 available at http://www.thehindubusinessline.com/todays-paper/tp-info-tech/article1643052.ece?ref=archive

[clxxxvii] DNA Investigations Bureau, Mumbai is number one for banking fraud in country, DNA, Jan. 8, 2011 available at http://www.dnaindia.com/mumbai/report_mumbai-is-number-one-for-banking-fraud-in-country_1634788 (last visited on 25/01/2012)

[clxxxviii] 'Spam capital' India arrests six in phishing probe, BBC, Jan. 3rd, 2012 available at http://www.bbc.co.uk/news/technology-16392960 (last visited on 25/01/2012)

clxxxix Mumbai Police unearth phishing racket, arrest six Nigerians, The Hindu, Jan. 3rd, 2012 available athttp://www.thehindu.com/news/states/other-states/article2769523.ece (last visited on 25/01/2012)

cxc Press Information Bureau. Cyber Crimes/Financial Frauds. Government of India. Available at: http://pib.nic.in/newsite/PrintRelease.aspx?relid=80936

cxci. "Guidelines for Technical and Financial Support for Establishment of State Data Centre", *Department of Electronics & Information Technology*, http://bit.ly/NQTCCu

cxcii. "Guidelines for Technical and Financial Support for Establishment of State Data Centre", s. 12.1., *Department of Electronics & Information Technology*.

cxciii. "Guidelines for Technical and Financial Support for Establishment of State Data Centre", ss. 13.1 and 14.1, *Department of Electronics & Information Technology*.

cxciv. "Guidelines for Technical and Financial Support for Establishment of State Data Center", *Department of Electronics & Information Technology*, http://bit.ly/NQTCCu

cxcv. Power Point presentation: CSC Seminar Presentations (2011). CSC Building Foundation for Rural Entrepreneurship. (2011).

cxcvi. See http://bit.ly/R7k94F

cxcvii. See http://bit.ly/aXDF4k

cxcviii . See http://bit.ly/aXDF4k

cxcix. Prashant Iyengar, "India Privacy Country Report", 2011, *Centre for Internet & Society*.

cc. "National Data Sharing and Accessibility Policy", *Government of India*, 2012, http://bit.ly/TX4cuo

cci . See http://bit.ly/eEfJw3

ccii. See http://bit.ly/UrrMlj

cciii. Mohanty, *supra* note___.

cciv. Ibid. Prashant Iyengar, "India Country Report".

ccv. "Kerala to be first fully digital State", *The Hindu*, June 5, 2012, http://bit.ly/Kt0j1w (last accessed on June 8, 2012).

ccvi. "Government to strengthen e-governance initiatives", *The Times of India*, June 7, 2012, http://bit.ly/OWZpJy (last accessed on June 8, 2012).

ccvii. "Speech by Honorable Prime Minister Shri Manmohan Singh at the inauguration ceremony of Indian Institute of Corporate Affairs Campus (13th April 2012 at IMT Manesar)", *Ministry of Corporate Affairs*, http://bit.ly/50Cri (last accessed on June 6, 2012).

ccviii. Pankaj Doval, "TCS, Infosys, Wipro vie for e-governance overhaul pie", *The Times of India*, June 4, 2012, http://bit.ly/M2d9OA (last accessed on June 8, 2012).

ccix. "Report of the Technology Advisory Group for Unique Projects" (TAGUP), *Ministry of Finance*, http://bit.ly/fItwhc (last accessed on January 31, 2012).

ccx. TAGUP Report, s. 10.2.

ccxi. TAGUP Report, s. 10.2.1.

ccxii. TAGUP Report, s. 10.2.2.

ccxiii. TAGUP Report, s. 10.2.3.

ccxiv. "Digitization of Land Records: Bhoomi Project", Government of Karnataka, http://bit.ly/93WaDC

ccxv India opening mail, tapping telephone, Leader-Post, Dec. 6, 1986, available at http://news.google.com/newspapers?id=X4lWAAAAIBAJ&sjid=Y0ENAAAAIBAJ&dq=phone%20tapping%20india&pg=3480%2C1703523 (last visited on Jan 23, 2012)