THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

Data Protection and Privacy Laws

Anjali Agarwal
4th year, BBA-LL.B, School of Law, Christ University, Bangalore, India

Abstract:
Cyber security is an emerging area of intense activity that endeavors to provide innovative solutions to ensure uninterrupted communications and service availability. Today, business is customer centric and success of any business depends on user's personal preference, in temptation to have technological adaptation, we outdo on our personal and some time sensitive information very easily without giving much concern to privacy. There no longer exists the freedom to refuse public information concerning personal data, but rather the freedom resides in the ability to control the use made of personal data inserted in a computer program which constitute the new right to privacy today. Ideally, the provided information must be used with limited purpose only for which it has been collected but in reality this information is further processed, transmitted and exploited for unauthorized purposes without the permission of data owner.
India does not at the time of publication have substantive legislation covering data protection in the workplace. However, the Indian Government has announced its intention to enact a new data protection regime which will help European and US Companies when outsourcing to the sub-continent. The National Association of Software and Service Companies (NASSCOM) is in the process of drafting legislation to amend the country's existing Information Technology Act, 2000 with an intention of bringing the data protection regime up to the standard required by the EU Directive.
There is a lack of apposite privacy legislation model so it is extremely difficult to ensure shield of privacy rights but, in the absence of specific laws there are some few proxy laws or incident safeguard that the government uses for privacy concern under the Constitution of India, IT Act 2000 and so on. The labour specific legislations of India do not contain any provision with respect to protection of employee data or privacy of employees. There is a growing need to protect sensitive employee, customer, and business data across the enterprise wherever such data may reside.
This research paper is an attempt to examine the data protection and privacy issues with special reference to India and attempt to determine the attribution factor in case of any violation.

1. Introduction

India is a Union of States[1] subdivided in twenty-nine States,[2] six Union Territories[3] and the National Capital Territory of Delhi. With a large vicinity and gigantic population, its service sector is demanding to keep pace with other sectors. While it provides a large number of legislation to govern all other sectors, the service sector is yet to develop in terms of privacy laws and regulations. The perception of data protection and privacy laws has not been addressed predominantly. India has no specific legislation or regulations concerning monitoring in the workplace. In contrast to the US, when Indian subjects are queried about the word *"privacy"*, the first thing that comes to their mind is privacy in terms of personal space and subjects, while the US subjects mention information privacy, financial information and identity theft.[4]

Privacy, as defined, is the *"claim of individuals, groups, or institutions to determine for themselves when, how and what extent information about themselves is communicated to others."*[5] Privacy is not an absolute concept[6]. With the technological developments, humans are now becoming technologically enhanced individuals, in essence cybernetic organisms. These technological enhancements facilitate everyday life, but at the same time create possible privacy violations.[7] The majority of the

[1] INDIA CONST. art. 1
[2] Andhra Pradesh, Arunachal Pradesh, Assam, Bihar, Chhattisgarh, Goa, Gujarat, Haryana, Himachal Pradesh, Jammu and Kashmir, Jharkhand, Karnataka, Kerala, Madhya Pradesh, Maharashtra, Manipur, Meghalaya, Mizoram, Nagaland, Orissa, Punjab, Rajasthan, Sikkim, Tamil Nadu, Telangana, Tripura, Uttaranchal, Uttar Pradesh, West Bengal
[3] Andaman and Nicobar Islands, Chandigarh, Dadra and Nagar Haveli, Daman and Diu, Lakshadweep and Pondicherry
[4] "48% of the subjects in India related privacy to physical, home and living space, but only 18% of the subjects in the US related privacy to these concepts", P. Kumaraguru and L. Cranor, " Privacy Perceptions in India and the United States : An Interview Study" at p. 6, (http://www.cs.cmu.edu/~ponguru/tprc_2005_pk_lc_en.pdf)
[5] S.K. Sharma, "Privacy Law: A Comparative Study" at p. 1
[6] R. Rajagopal v. State of Tamil Nadu, (1994) 6 S.C.C. 632, 639
[7] Natasha Vaz ,"Identity, Minorities, Social Networking and Privacy", April 30, 2012 at http://privacy-india.org/

population are not aware of the technical know how of the upcoming technologies which are advancing at a fast pace. Not all people are able to keep up with the same pace, making the laws in this sector week to a great extent.

The objective of Privacy are, as stated by Prashant Iyengar, is *"to raise awareness, spark civil action and promote democratic dialogue around privacy challenges and violations in India. One of Privacy India's goals is to build consensus towards the promulgation of comprehensive privacy legislation in India through consultation with the public, legislators and the legal and academic community."*[8]

With introduction of various technologies it became difficult to protect the information through confidentiality only and the coverage of protection has been widen to include integrity and availability so as to achieve information security. With advancement of latest technology for which many efforts at technological and legal level are done but still there is threat to information because the scope of privacy has been remain still untouched and to provide complete protection to information it is essential to cover the privacy. Although the digitization of data has created convenience in terms of availability yet it has created havoc of data overflow that leads to difficulty in management of large data, it also includes personal and sensitive information like credit card information. Improper handling of this data can create damage and loss for individual as well Nation.[9]

Today, business is customer centric and success of any business depends on user's personal preference, in temptation to have technological adaptation, we outdo on our personal and some time sensitive information[10] very easily without giving much concern to privacy. For example, from creating a mail account to open an online banking account we pass on our personal information everywhere in day to day life. Ideally, the provided information must be used with limited purpose only for which it has been collected but in reality this information is further processed, transmitted and exploited for unauthorized purposes without the permission of data owner.[11] In Indian context, there is a lack of pertinent privacy legislation model so it is extremely difficult to ensure shield of privacy rights.[12]

2. Whether the Present Legislation in India Shielding the Personal Information and Workplace Data Adequate?

Unlike the physical world that has clearly defined geographical boundaries, cyberspace is borderless, and with increased Internet penetration, it's becoming larger since its size is proportionate to the activities carried out in it.[13] Buying and selling of goods or services(like e commerce), transfer of funds through banks, making credit card payments, sending emails, interfacing with people through social networking sites and exchanges of pictures, videos or music are some activities performed in cyberspace. There is, thus, a seamless merging of cyberspace with the physical world[14] and clearly of crime also. It is also used as a medium to exchange information for carrying out financial frauds and terrorist activities in the physical world.

Personal information is defined as the information which is related or regarding to an identifiable or identified identity of a natural person.[15] It may be referred to as personal data, personal information, non-public information, etc. and includes Name, Address, Date of Birth, Telephone Number, Fax Number, Email Address, Government Identifier (e.g. PAN Number, PF account number, etc.), Account Number (Bank Account, Credit Card, etc.), Driving License Number, IP Address, Biometric Identifier,[16] Photograph or Video Identifiable to an Individual and any other unique identifying number, characteristic or code. [17]

The impact of globalization on privacy of identity is growing. The fact that more and more personal information is crossing borders in trans-border data flows means that data breaches often affect people in multiple countries, and may result in financial frauds as in the case of TJX Companies Inc., a retailer in the US. Nearly 100 million credit and debit cards belonging to people from various regions were exposed when hackers broke into its computer systems[18]

2.1. Privacy

The tern privacy and right to privacy cannot be easily conceptualized. In modern society privacy has been recognized both in the eye of the law and in common parlance. Privacy is a neutral relationship between persons or groups or between groups and persons. Privacy is a value, a culture state or condition directed towards individual on collective self realization varying from society to society.

---

[8]Natasha Vaz,,"Privacy: RTI, UID and Surveillance", April 29, 201 at_http://privacy-india.org/2012/04/29/privacy-rti-uid-and-surveillance/

[9] Privacy-Enhancing Technologies: Approaches and Development http://www.sciencedirect.com/ , (Last seen on 18/15/2010)

[10] Section 2(1)(v) of Information technology Act, 2000

[11] Privacy-Enhancing Technologies: Approaches and Development http://www.sciencedirect.com/ , (Last seen on 18/15/2010)

[12]Ponnurangam Kumaraguru, "Privacy in India: Attitudes and Awareness" at http://www.cs.cmu.edu/~ponguru/iaap_nov_2005.pdf

[13]Kamlesh Bajaj, "The Cybersecurity Agenda: Mobilizing for International Action", at http://www.ewi.info/system/files/Bajaj_Web.pdf

[14]http://www.digitalopportunity.org/comments/amendments-to-it-act-tighten-cyber-security (Last seen on 12/14/10)

[15] Kamlesh Bajaj Chief Executive Officer, DSCI, "Data Protection - Security and Privacy Cyber Society of India", 13 Feb 2010.

[16]Unique Identification Authority of India Planning Commission, Government of India at http://uidai.gov.in/what-is-aadhaar-number.html

[17]Kamlesh Bajaj Chief Executive Officer, DSCI, "Data Protection - Security and Privacy Cyber Society of India", 13 Feb 2010.

[18] Kamlesh Bajaj, http://www.livemint.com/2009/01/18235959/Stringent-data-protection-law.html (Last seen on 12/14/10)

The Constitution of India does not specifically recognize the right to privacy.[19]The Indian Constitution in Article 19 (1) (a)[20] provides the right to freedom of speech and expression[21], which implies that a person is free to express his will about certain things. A person has freedom of life and personal liberty, which can be taken only by procedure established by law under Article 21.[22] These provisions improvably provide right to privacy to individuals and/or groups of persons.[23] The personal liberty in Article 21 is of the widest amplitude and it covers a variety of rights which constitute the personal liberty,[24] secrecy,[25] autonomy,[26] human dignity,[27] human right,[28] self evaluation, limited and protected communication,[29] limiting exposure[30] of man and some of them have been raised to the status of fundamental rights.[31] Privacy relates to ability to control the dissemination and use of one's personal information.[32] The Supreme Court of India, has noted that right to privacy[33] was an *"essential ingredient of personal liberty"* which is *"a right to be free from restrictions or encroachments"*[34] indication that there is a right of privacy implicit in the Constitution,[35] which provides: *"No person shall be deprived of his life or personal liberty except according to procedure established by law."* [36] There should be more reliance on the self-regulation of businesses that promote practices, making the privacy program relevant to technology advancements and having the legal recognition for the same.[37]

Indian government is instrumental towards e-surveillance since the pressure from the industrial bodies for weak and ineffective cyber laws is costing Indians their privacy and data protection law. The truth is that privacy rights in India are at stake. The e-surveillance projects include unique identification project of India (UID project) or Aadhar project of India managed by Nandan Nilekani as the chairman of unique identification authority of India (UIDAI).[38] Other projects include national intelligence grid (Natgrid), CCTNS, etc.[39] IT Act 2000 is the sole cyber law of India that has been made an instrumentality of e surveillance by Indian government. Further, under pressure from industrial bodies, almost all the cyber crimes have been made bailable. However, the gravest of all concerns is the high level of e-surveillance in India with no corresponding privacy laws, data protection laws and procedural safeguards. Even the IT Act 2000 is silent on the procedural safeguards against illegal and unconstitutional e-surveillance, internet censorship, etc.

The government is proposing legislation that will empower citizens with sweeping rights to legal recourse against any misuse of personal data. The first draft of the proposed legislation has been released for public debate by the department of personnel and training (DoPT).[40] The umbrella legislation aims at a situation where the confidential personal information disclosed by any individual is not revealed to third parties without the person's consent. The legislation will ensure that sufficient safeguards are adopted in the process of collecting, processing and storing such information.

---

[19] Pooran Mal v. Director of Inspection (Investigation) of Income-tax, New Delhi, AIR 1974 SC 348; State of Punjab v. Baldev Singh, AIR 1999 SC 2378; R. Rajagopal v State of Tamil Nadu, AIR 1995 SC 264; Peoples Union for Civil Liberties (PUCL) v. Union of India, AIR 2003 SC 2363; X v. Hospital Z AIR. 1999 SC 495; Sharda v. Dharmpal, AIR 2003 SC 3450; District Registrar and Collector v. Canara Bank, (2005)1 SCC 496

[20] "All citizens shall have the right to freedom of speech and expression …"

[21] Gobind v. State of Madhya Pradesh, 1975 AIR 1378

[22]"No person shall be deprived of his life or personal liberty except according to procedure established by law."

[23] People's Union of Civil Liberties v the Union of India, (1997) 1 SCC 318

[24] Samuel Warren & Louis D. Brandeis, "The Right to Privacy" (1890) 4 no. 5 Harv L. Rev 193

[25] Kharak Singh v. State of U.P, AIR 1963 SC 1295

[26] Allgeyer v. State of Louisiana, 41 L Ed. 832

[27] Louis Henkin, "Privacy and Autonomy" (1974) 74 Columbia Law review 1410

[28] Oimstead v. United States, 72 l.Ed. 944

[29] Article 12 of the Universal Declaration of Human Rights, 1948; Article 17 of the International Covenant of Civil and Political Rights, 1966

[30] Westlin, Alan F, "Science, Privacy and Freedom", (1966) 66 Columbia Law Review 1003

[31] Madhavi Divan, The Right to Privacy in the Age of Information and Communications, 4 SCC (Jour) (2002), available at http://www.ebc-india.com/lawyer/articles/2002v4a3.

[32] Dr. Shiv Shankar Singh, Privacy and data Protection in India, (2012) PL February S-2

[33] V.S. Kuttan Pillai v. Ramakrishnan, AIR 1980 SC 185

[34] U.S. Dep't of Commerce, "Privacy and the NII: Safeguarding Telecommunication-related Personal Information" 5 (1995), at http://www.ntia.doc.gov/ntiahome/provwhitepaper.html.

[35] Constitution of India,.Art. 21.

[36] INDIA CONST. art. 21; M. P. Sharma v. Satish Chandra, District Magistrate, Delhi AIR 1954 SC 300

[37] Madeleine Schachter, "Informational and decisional privacy", Carolina Academic Press, 2003 at 210

[38]Priyanka Sharma, " Data Protection Law in India is Uregently Required" at http://cyberlawsinindia.blogspot.in/2010/10/data-protection-law-in-india-is.html (Last seen on 30/10/2010)

[39]Priyanka Sharma, " Data Protection Law in India is Uregently Required" at http://cyberlawsinindia.blogspot.in/2010/10/data-protection-law-in-india-is.html (Last seen on 30/10/2010)

[40]Surabhi Aggarwal, "Legal Action on Personal Data Misuse", at http://www.livemint.com/2010/11/21231138/Legal-action-on-personal-data.html , (Last seen on 12/10/2010)

2.2. Data Protection

Data protection refers to the issues related to the collection, storage, accuracy and use of data[41] provided by net users in the use of the World Wide Web. Visitors to any website want their privacy rights to be respected when they engage in any transaction. It is part of the confidence creating role that successful e-commerce business has to convey to the consumers.[42]

Any transaction between two or more parties[43] involves an exchange of essential information[44] between the parties. Technological developments have enabled transactions by electronic means. Any such information[45]/data[46] collected by the parties should be used only for the specific purposes for which they were collected. The need arose, to create rights for those who have their data stored and create responsibilities for those who collect, store and process such data. The law[47] relating to the creation of such rights and responsibilities may be referred to as "data protection" law.

Thus, data protection is a type of privacy protection manifesting in special legal regulation. Data protection right ensures a person the right of disposal over all data in connection with his personality. This way it serves to sustain the protection of privacy in a world where the possibility of collecting, storing and conciliation of large pools of data is widely available.

The protection of data[48] finds its roots in the individual's right to privacy doctrine.[49] However, a right under the Constitution can be exercised only against any government action. Non-state initiated violations of privacy[50] may be dealt with under principles of torts[51] such as defamation, trespass and breach of confidence, as applicable.[52]

The definition of "data"[53] and its protection in the Indian context, does not give a comprehensive understanding of the term. *"Data protection refers to the set of privacy-motivated laws, policies and procedures that aim to minimize intrusion into respondents' privacy caused by the collection, storage and dissemination of data."*[54] The IT Act doesn't provide for any definition of personal data. Furthermore, the definition of "data" would be more relevant in the field of cybercrime.[55] This law is unlikely to be applied to workplace monitoring, as it has no direct application to such monitoring. Instead, the Act is intended to provide a comprehensive regulatory environment for electronic commerce. The Act makes punishable cyber crimes like hacking,[56] damage to computer source code,[57] and breaches of confidentiality and privacy.[58]

3. Existing Legislation in India Governing Privacy and Data Protection

Discussing the provisions, Section 43A[59] provides for the protection of sensitive personal data or information ('SPDI')[60] and Section 43(b)[61] affords cursory safeguards against breaches in data protection. The scope of Section 43(b) is limited to the unauthorized access, downloading, copying, extraction, or damage of data from a computer system.[62]

However, the Information Technology (Amendment) Act of 2008 has removed any cap on the amount of damages.[63] The damages under Section 43[64] were quantified at Rupees one crore, but the IT Act of 2008 has removed this limit of one crore and made the

---

[41] Section 2(1)(o) of Information Technology Act, 2000

[42] Dr S S Das, "Electronic Data Protection In India", 2012 PL March S-11

[43] Section 2(1)(w) of Information Technology Act, 2000

[44] Section 2(1)(v) of Information Technology Act, 2000

[45] Section 2(1)(v) of Information Technology Act, 2000

[46] Section 2(1)(o) of Information Technology Act, 2000

[47] Section 2(1)(y) of Information Technology Act, 2000

[48] Section 2(1)(o) of Information Technology Act, 2000

[49] Peter Carey, "Data Protection: A Practical Guide to UK and EU Law", 23 (2d ed. 2004)

[50] Sagarika Ghose, "Controversy Of Love And Libel", at http://www.outlookindia.com/article.aspx?200468

[51] R. Rajagopal v. State of Tamil Nadu, (1994) 6 S.C.C. 632, 639

[52] Ian J. Turnbull, "Privacy in the Workplace", CCH Canadian Limited, 2009, 2nd ed. at 93

[53] Section 2(1)(o) of Information Technology Act, 2000, *"representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;"*

[54] Organisation for Economic Co-Operation and Development, Data Protection, Glossary of Statistical Terms, http://stats.oecd.org/glossary/detail.asp?ID=%206903

[55] Article 12, Universal Declaration of Human Rights, 1948 at http://www.ohchr.org/EN/UDHR/Documents/UDHR Translations/eng.pdf

[56] Section 66 of Information Technology Act, 2000

[57] Section 65 of Information Technology Act, 2000

[58] Section 72 of Information Technology Act, 2000

[59] "Compensation to failure to protect Data", Information Technology (Amendment) Act, 2008

[60] Section 43A .Cl.(iii) of Information Technology Act, 2000

[61] "downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;"

[62] Section 43of Information Technology Act, 2000

[63] Section 43A of Information Technology Act, 2000

[64] "Penalty for damage to computer, computer system, etc" Information Technology Act, 2000

damages unliquidated. Thus, this interprets that the damages[65] that one can suffer under these instances can be well above Rupees one crore.[66]

Section 72A[67] protects personal information from unlawful disclosure in breach of contract. Tampering with computer source documents and Hacking with computer system[68] is dealt under Section 65[69] and Section 66[70] respectively. Apart from these provisions, the IT Act does not show any guiding light in the matters concerned.

The government has freshly introduced certain rules ('Rules')[71] under the IT Act which, read along with section 43A, 65, 66, and 72 set out the compliances which need to be observed by an entity which collects or stores or otherwise deals with SPDI (such as passwords, financial information, health conditions, physical, physiological, sexual orientation, medical records and biometric records and so on). The Privacy Rules[72] also do not specifically address workplace monitoring. It has however, attempted to tackle the issue of data protection and privacy.[73]

The Privacy Rules[74] prescribe restrictions on the transfer of data. Any such transfer must be undertaken only with the consent of the data subject and only if necessary for the performance of a contract. At all times, sensitive personal data or information must be transferred only to another corporate entity that ensures the same level of data protection.

In the BPO sector, a central employee database has been created by the National Association of Software and Service Companies (NASSCOM). This registry endeavors to house updated information on employees working in the IT and BPO sector. The media has reported that this employees in the IT and BPO industries will be required to join this registry.

To implement privacy and data protection in Indian work culture, government has established DSCI (Data Security Council of India) which was initiative by NASCCOM.[75]Its mission is to create trustworthiness of Indian company as global sourcing service provider. Its main aim is to create privacy and security awareness among organization.

In this backdrop, the judgment of the Delhi State Consumer Disputes Redressel Commission (the "Commission"), which imposed a total fine of Rs.75 lakhs on Airtel, the Cellular Operators Association of India ("COAI"), ICICI Bank and American Express Bank on a complaint of consumer harassment by unsolicited telemarketing calls and text messages assumes enormous significance.[76] In 1997, the Supreme Court of India directed the Reserve Bank of India ("RBI") to institute to implement measures to reduce unsolicited calls on the ground that the right to privacy is a fundamental right.[77]

Recently, India has adopted Right to Information (RTI) which talks about disclosure of public information when required. It is observed that RTI is an encroachment of Personal information. For successful implementation of RTI it is required to define the Privacy, information classification so that it can help to disclose the information without impairment of routine work.[78]

According to the Indian Contract Act, when a party commits a breach of contract, the other party is entitled to receive compensation for any loss or damage caused to it, or, in exceptional cases, the court may direct the "specific performance" of the contract against the party in default.[79] Hence, Indian companies acting as 'data importers' may enter into contracts with 'data exporters' to adhere to a high standard of data protection.[80] These contracts are binding and may fulfill the requirements of overseas customer(s) national legislations. Moreover, increasingly, outsourcing/BPO contracts are also incorporating clause(s) on international arbitration for dispute resolution.[81] Furthermore, Indian outsourcing/BPO companies are accepting that the governing law under the Agreement(s) and any action arising hereunder shall be construed in accordance with and be governed by the substantive and procedural laws of the customer's national laws without regard to the conflict of law's provisions thereof.[82] They

---

[65] Section 43A of Information Technology Act, 2000

[66] Section 43A of Information Technology Act, 2000

[67] "Punishment for Disclosure of Information in Breach of Lawful Contract", Information Technology (Amendment) Act, 2008

[68] Section 2(1) (k) of Information Technology Act, 2000

[69] "Tampering with computer source documents", Information Technology Act, 2000

[70] "Hacking with computer system.", Information Technology Act, 2000

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

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

[73] NASSCOM Announces Milestones for Its 'Trusted Sourcing' Initiative, NASSCOM

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

[75]DSCI Excellence Awards 2011 at http://www.dsci.in/sites/default/files/PR_DSCI%20Excellence%20Awards_post.pdf on 22/07/2011

[76] Anoop Narayanan, "Protection of personal data", The Economic Times at http://articles.economictimes.indiatimes.com/2007-01-29/news/27669329_1_privacy-personal-information-icici-bank (Last seen on 29/01/2007)

[77] Vakul Sharma, " White Paper on Privacy Protection in India", at http://www.iamai.in/Upload/IStandard/White%20Paper%20on%20Privacy.%202007.pdf , http://www.majmudarindia.com,

[78] Ms. M. Shanthi, "News on Right to Information" at www.rti.org.in

[79] Section 73of Indian Contract Act, 1872

[80] Subhajit Basu, "Policy-Making, Technology And Privacy In India", The Indian Journal Of Law And Technology, Volume 6, 2010 at http://www.ijlt.in/archive/volume6/3.pdf

[81]CRID,"First Analysis of the Personal Data protection Law in India",University of Namur at http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_india_en.pdf

[82]CRID,"First Analysis of the Personal Data protection Law in India",University of Namur at http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_india_en.pdf

are also submitting themselves to the exclusive jurisdiction of customer's national courts and forums.[83] In some cases, Indian outsourcing/BPO companies are also accepting process of mediation to resolve the dispute. For example, companies are agreeing to dispute resolution by non binding mediation under the International Mediation Rules of the International Centre for Dispute Resolution of the American Arbitration Association ("ICDR").

Finally, some Indian IT companies like WIPRO, INFOSYS, TCS, active in the IT/ BPO sector presently have a very stringent policy dealing with protection of their client's information and all the employees are contractually bound to protect the confidential information which may be processed. The employment contracts clearly specify that the employees have to maintain as secret and confidential all such information which the company specifies from time to time[84]. From all these examples, one could claim that on an informal basis, there are attempts being made by Indian companies to ensure privacy of data although in many cases it may not be dealing specifically personal data.

The Credit Information Companies (Regulation) Act, 2005 was passed with a view to regulate credit information companies and to facilitate efficient distribution of credit and for matters concerned or incidental to it. The Credit Information Companies (Regulation) Act of 2005 "imposes duties on credit information companies, credit institutions, and specified users while processing credit data.[85] Additionally, the Reserve Bank of India has the authority to penalize any credit information company, credit institution, or specified user, for violating this Act.[86] On this ground, the "Reserve Bank of India could be considered as a specific data protection authority in the field of credit information."[87]

With the phasing out of the traditional means of data retention in physical paper form like telephone directories, yellow pages and instead a switch to data being retained in electronic form, it has become easier for a person to copy the data of another and distribute the same for commercial gain. With the absence of a specific legislation on database, companies have to rely on the interpretation of the Copyright Act by the courts, especially those pertaining to how database is a literary work and thus protected under the Copyright Act. Computer software (including computer programs[88], databases, computer files, preparatory design material, and associated printed documentation, such as users' manuals)[89] receives copyright protection under Indian laws.[90] The Indian Copyright Act of 1957 "prescribes mandatory punishment for piracy of copyrighted matter commensurate with the gravity of the offense."[91] Computer programs are not per se patentable, being patentable only in combination with hardware.[92]Thus in India, by past practice and under current laws, copyright is the preferred mode of protection for computer software as it is considered as a literary work.[93]In the case of V. Govindan v. E.M Gopalakrishna[94] the court held that the Copyright Act only protects slavish imitation of data.This interpretation would not adequately check the menace of copying another person's database with slight modifications.

---

[83]CRID,"First Analysis of the Personal Data protection Law in India",University of Namur at http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_india_en.pdf

[84] Following is the provisions dealing with confidentiality in the employment contract of a leading Indian IT company WIPRO :

"In consideration of the opportunities training and access to new technologies and know how that will be made to you, you will be required to comply with the confidentiality policy of the company. Therefore please ensure that you maintain as secret and confidential all Confidential Information (as defined from time to time in the confidentiality policy of the company) and shall not use or divulge or disclose any such Confidential Information except as may be required under obligation of law or as may be required by WIPRO and in the course of your employment. The covenant shall endure during your employment and for a period of one year from the cessation of your employment with WIPRO (irrespective of the circumstances of, or the reasons for, the cessation) In your work for WIPRO, you will be expected not to use or disclose any confidential information, including trade secrets, of any former employer or other person with whom you have an obligation of confidentiality and by signing below you affirm that you have no conflicting obligations or non-compete agreements that would prevent you from working without limitation for WIPRO Technologies"

[85] Rodney D. Ryder & Ashwin Madhavan,, "Data Protection, Privacy and Corporate Compliance: The Law and Emerging Trends in India" at http://information5.com/d/data-protection,-privacy-and-corporate-compliance-the-law-and-w3109.html

[86] Rodney D. Ryder & Ashwin Madhavan, "Data Protection, Privacy and Corporate Compliance: The Law and Emerging Trends in India",at http://information5.com/d/data-protection,-privacy-and-corporate-compliance-the-law-and-w3109.html

[87] Rodney D. Ryder & Ashwin Madhavan, "Data Protection, Privacy and Corporate Compliance: The Law and Emerging Trends in India", at http://information5.com/d/data-protection,-privacy-and-corporate-compliance-the-law-and-w3109.html

[88] Section 63B of the Indian Copyright Act of 1957

[89] Burlington Home Shopping v. Rajnish Chibber 61 (1995) DLT 6

[90] Section 2(o) of the Indian Copyright Act of 1957

[91]Umesh Pandit, "Intellectual Property Rights in India", knol Beta, at http://knol.google.com/k/umeshpandit/intellectual-property-rights-in-india/r0tyv5xaaisc/45#

[92] Manisha Singh, "India's Patent law - is it TRIPs compliant?" (2005) at http://www.managingip.com/article/1321451/Indias-patent-lawis-it-TRIPs-compliant.html.

[93] Eastern Book Company v. D.B. Modak [Appeal (Civil) 6472 of 2004]

[94] AIR 1955 Mad 391

Under the Indian Penal Code of 1860 ("IPC"), there is no express criminal punishment for breaching data privacy. Thus "liability for data-related breaches must be inferred from tangentially related crimes."[95]For example, "Section 403 of the Indian Penal Code imposes criminal penalty for dishonest misappropriation or conversion of 'movable property' for one's own use."[96] Therefore, "although no jurisprudence has been developed on this interpretation, arguably, movable[97] property encompasses computer-related data and intellectual property."[98]

There is an element of trust involved when a person discloses his or her personal information to another. In the case where this information is disclosed to a third party, it could result in criminal penalties for the criminal breach of trust.[99]Further, the IPC imposes criminal liability for dishonest or fraudulent concealment or removal of property[100], and also for when a person "cheats and thereby dishonestly induces the person" in possession of the property to deliver the said property.[101]Furthermore, section 425 imposes liability on a third party who intends to cause wrongful loss[102] or damage to the property of another person, whether or not the person is the owner of the property.[103]

Upon the footprints of the foreign laws, The Personal Data Protection Bill, 2006 has been introduced in the Rajya Sabha on December 8th 2006. The purpose of this bill is to provide protection of personal data and information of an individual collected for a particular purpose by one organization, and to prevent its usage by other organization for commercial or other purposes and entitle the individual to claim compensation or damages due to disclosure of personal data or information of any individual without his consent and for matters connected with the Act or incidental to the Act. The Bill was drafted wholly on the structure of the UK Data Protection Act. But this proposed Act has lapsed now.

The Privacy Bill, 2011, aims at "safeguarding the security interests of all affected individuals in the personal data that has or is likely to have been compromised by such a breach".[104] The Bill proposes a maximum punishment of five years and/or fine of Rs 7 lakh for the first offence and Rs 10 lakh for every subsequent offence.[105] The proposed law also aims to empower an individual or group of individuals to take legal recourse to protect the "confidentiality of his private or family life"; seek protection from "search, detention or exposure of lawful communication": have privacy from surveillance: ensure confidentiality of his banking and financial transactions as well as his/her medical and legal information. The Requisitioning Service Agency (Government) and the Service Provider (the Telecommunications Company or the ISP) are bodies set up under the proposed law. Each has been required to appoint nodal officers and the transaction of exchange of any information collected shall occur only between them. Strict guidelines are provided for such exchange, as the same has been asked to follow a method of exchanging appropriate acknowledgement letters, etc. Further, the Service Providers have been placed with responsibility, as they have to every fifteen days submit a list of authorizations, to the Security agencies for confirmation of authenticity of the directions received by them[106]. Further, stipulations are provided with respect to secrecy, maintenance of data, destruction of records etc. This will check unauthorized tap orders purportedly emanating from government as noticed in the recent decision of Amar Singh v. Union of India[107].

The Data Protection Authority of India has been set up as a regulatory body to administer the Privacy.[108]National Data Controller Registry, this is in the form of an online database in order to facilitate the efficient and effective entry of particulars by data controllers. A data controller has the permission to process any personal data of any data subject, only after the data controller has made an entry in the registry.

Cyber Regulations Appellate Tribunal which is established under Section 48 of the Information Technology Act, 2000[109] has the original jurisdiction with respect to any dispute arising between an individual and a data controller and appellate jurisdiction with respect to any appeal from any order or direction or decision of the Authority [Data Protection Authority of India]. It is of interest that this Appellate Tribunal through this Bill will be given original jurisdiction where earlier it only sat as a court of appeal. [110]

Telegraph Act of 1885, amended in 2004, regulates certain public telecommunications.[111] Prevention of Terrorism Act of 2002[112] limits terrorists' privacy rights. The pending Right of Information Bill of 2004, a proposal that is the closest India would come to a comprehensive privacy law, is broad but would reach only public institutions.[113]

---

[95] Vinita Bali, "Data Privacy, Data Piracy: Can India Provide Adequate Protection for Electronically Transferred Data?" , Santa Clara University School of Law, Oct. 2006

[96] Section 403of India Penal Code

[97] Section 22 of Indian Penal Code

[98]Manisha Singh, "India's Patent law - is it TRIPs compliant?" (2005) at http://www.managingip.com/article/1321451/Indias-patent-lawis-it-TRIPs-compliant.html

[99]Section 405 of Indian Penal Code

[100] Section 424 of Indian Penal Code

[101] Section 420 of Indian Penal Code

[102] Section 23 of Indian Penal Code

[103] Section 425of Indian Penal Code

[104] Ministry of Personnel, Public Grievances & Pensions, Right to Privacy Bill, 2011

[105] Section 78 of the Privacy Bill, 2011

[106] Section 5(2) of the Indian Telegraph Act, 1885

[107] (2011) 7 SCC 69

[108] Section 6(2) of Right to Privacy Bill, 2011

[109] Section 2(n) of Information Technology Act, 2000

[110] Section 48 of Information Technology Act, 2000

[111] Indian Telegraph (Amendment) Rules, 2004 at www.dot.gov.in/Acts/rules.doc

[112]Prevention of Terrorism Act, 2002 at www.satp.org/satporgtp/countries/india/document/actandordinances/POTA.htm

In spite of various legislations there is no comprehensive substantive legislation dealing with privacy and data protection specifically.

4. Conclusion

Privacy is a basic human right and computer systems contain large amount of data that may be sensitive. The Information Technology Act defines liabilities for violation of data confidentiality and privacy related to unauthorized access to computer, computer system, computer network or resources, unauthorized alteration, deletion, addition, modification, destruction, duplication or transmission of data, computer database, etc. The data protection may include financial details, health information, business proposals, intellectual property and sensitive data.

However, today we can access many information related to anyone from anywhere at any time but this poses a new threat to private and confidential information. Globalization has given acceptance to technology in the whole world and different countries have introduced different legal framework like Data Protection Act, 1998 of UK, Electronic Communication Privacy Act, 1986 of USA, etc. from time to time.

The right to privacy is recognized in Indian Constitution but its growth and development is entirely left at the mercy of the judiciary. In today's connected world it is very difficult to prevent information to escape into the public domain if someone is determined to put it out without using extremely repressive methods. Data protection and privacy has been dealt with in the Information Technology Act, 2000 but not in an exhaustive manner, The IT Act needs to establish setting of specific standards relating to the methods and purpose of assimilation of right to privacy and personal data. We may conclude by saying that the IT Act is facing the problem of protection of data and a separate legislation is much needed for data protection striking an effective balance between personal liberties and privacy.

The Indian Information Technology Act reaffirms India's commitment towards building a knowledge-based society and keeping in pace with the rest of the world by providing a legal framework within which such society can flourish. While the Indian Government has taken its first step in regulating the cyber crimes by passing the IT Act 2000, the legal regime on Information Technology in India is still in its nascent stage. Following the footsteps of United States and EU which have adopted specific legislations for data protection and privacy, India Government is also in the process of formulating laws to tighten its legal regime over the issues relating to data protection and privacy to bolster its offshore credibility. The government has taken into account the modern ways of violation of data protection norms and issues relating to electronic contracts breach of confidentiality and privacy, in order to bring a comprehensive legislation to protect the rights of the netizens. This will go a long way in making Internet and cyber space safer, people friendly and commercially more viable.

5. References

1. INDIA CONST. art. 1
2. Andhra Pradesh, Arunachal Pradesh, Assam, Bihar, Chhattisgarh, Goa, Gujarat, Haryana, Himachal Pradesh, Jammu and Kashmir, Jharkhand, Karnataka, Kerala, Madhya Pradesh, Maharashtra, Manipur, Meghalaya, Mizoram, Nagaland, Orissa, Punjab, Rajasthan, Sikkim, Tamil Nadu, Telangana, Tripura, Uttaranchal, Uttar Pradesh, West Bengal
3. Andaman and Nicobar Islands, Chandigarh, Dadra and Nagar Haveli, Daman and Diu, Lakshadweep and Pondicherry
4. "48% of the subjects in India related privacy to physical, home and living space, but only 18% of the subjects in the US related privacy to these concepts", P. Kumaraguru and L. Cranor, " Privacy Perceptions in India and the United States : An Interview Study" at p. 6, (http://www.cs.cmu.edu/~ponguru/tprc_2005_pk_lc_en.pdf)
5. S.K. Sharma, "Privacy Law: A Comparative Study" at p. 1
6. R. Rajagopal v. State of Tamil Nadu, (1994) 6 S.C.C. 632, 639
7. Natasha Vaz ,"Identity, Minorities, Social Networking and Privacy", April 30, 2012 at http://privacy-india.org/
8. Natasha Vaz,,"Privacy: RTI, UID and Surveillance", April 29, 201 at http://privacy-india.org/2012/04/29/privacy-rti-uid-and-surveillance/
9. Privacy-Enhancing Technologies: Approaches and Development http://www.sciencedirect.com/, (Last seen on 18/15/2010)
10. Section 2(1)(v) of Information technology Act, 2000
11. Privacy-Enhancing Technologies: Approaches and Development http://www.sciencedirect.com/ , (Last seen on 18/15/2010)
12. Ponnurangam Kumaraguru, "Privacy in India: Attitudes and Awareness" at http://www.cs.cmu.edu/~ponguru/iaap_nov_2005.pdf
13. Kamlesh Bajaj, "The Cybersecurity Agenda: Mobilizing for International Action", at http://www.ewi.info/system/files/Bajaj_Web.pdf
14. http://www.digitalopportunity.org/comments/amendments-to-it-act-tighten-cyber-security (Last seen on 12/14/10)
15. Kamlesh Bajaj Chief Executive Officer, DSCI, "Data Protection - Security and Privacy Cyber Society of India", 13 Feb 2010.
16. Unique Identification Authority of India Planning Commission, Government of India at http://uidai.gov.in/what-is-aadhaar-number.html

[113]Right to Information Bill, 2004 at www.humanrightsinitiative.org/programs/ai/rti/india/national/rti_bill_2004_tabled_version.pdf

17. Kamlesh Bajaj Chief Executive Officer, DSCI, "Data Protection - Security and Privacy Cyber Society of India", 13 Feb 2010.
18. Kamlesh Bajaj, http://www.livemint.com/2009/01/18235959/Stringent-data-protection-law.html (Last seen on 12/14/10)
19. Pooran Mal v. Director of Inspection (Investigation) of Income-tax, New Delhi, AIR 1974 SC 348; State of Punjab v. Baldev Singh, AIR 1999 SC 2378; R. Rajagopal v State of Tamil Nadu, AIR 1995 SC 264; Peoples Union for Civil Liberties (PUCL) v. Union of India, AIR 2003 SC 2363; X v. Hospital Z AIR. 1999 SC 495; Sharda v. Dharmpal, AIR 2003 SC 3450; District Registrar and Collector v. Canara Bank, (2005)1 SCC 496
20. "All citizens shall have the right to freedom of speech and expression …"
21. Gobind v. State of Madhya Pradesh, 1975 AIR 1378
22. "No person shall be deprived of his life or personal liberty except according to procedure established by law."
23. People's Union of Civil Liberties v the Union of India, (1997) 1 SCC 318
24. Samuel Warren & Louis D. Brandeis, "The Right to Privacy" (1890) 4 no. 5 Harv L. Rev 193
25. Kharak Singh v. State of U.P, AIR 1963 SC 1295
26. Allgeyer v. State of Louisiana, 41 L Ed. 832
27. Louis Henkin, "Privacy and Autonomy" (1974) 74 Columbia Law review 1410
28. Oimstead v. United States, 72 l.Ed. 944
29. Article 12 of the Universal Declaration of Human Rights, 1948; Article 17 of the International Covenant of Civil and Political Rights, 1966
30. Westlin, Alan F, "Science, Privacy and Freedom", (1966) 66 Columbia Law Review 1003
31. Madhavi Divan, The Right to Privacy in the Age of Information and Communications, 4 SCC (Jour) (2002), available at http://www.ebc-india.com/lawyer/articles/2002v4a3.
32. Dr. Shiv Shankar Singh, Privacy and data Protection in India, (2012) PL February S-2
33. V.S. Kuttan Pillai v. Ramakrishnan, AIR 1980 SC 185
34. U.S. Dep't of Commerce, "Privacy and the NII: Safeguarding Telecommunication-related Personal Information" 5 (1995), at http://www.ntia.doc.gov/ntiahome/provwhitepaper.html.
35. Constitution of India,.Art. 21.
36. INDIA CONST. art. 21; M. P. Sharma v. Satish Chandra, District Magistrate, Delhi AIR 1954 SC 300
37. Madeleine Schachter, "Informational and decisional privacy", Carolina Academic Press, 2003 at 210
38. Priyanka Sharma, " Data Protection Law in India is Uregently Required" at http://cyberlawsinindia.blogspot.in/2010/10/data-protection-law-in-india-is.html (Last seen on 30/10/2010)
39. Priyanka Sharma, " Data Protection Law in India is Uregently Required" at http://cyberlawsinindia.blogspot.in/2010/10/data-protection-law-in-india-is.html (Last seen on 30/10/2010)
40. Surabhi Aggarwal, "Legal Action on Personal Data Misuse", at http://www.livemint.com/2010/11/21231138/Legal-action-on-personal-data.html , (Last seen on 12/10/2010)
41. Section 2(1)(o) of Information Technology Act, 2000
42. Dr S S Das, "Electronic Data Protection In India", 2012 PL March S-11
43. Section 2(1)(w) of Information Technology Act, 2000
44. Section 2(1)(v) of Information Technology Act, 2000
45. Section 2(1)(v) of Information Technology Act, 2000
46. Section 2(1)(o) of Information Technology Act, 2000
47. Section 2(1)(y) of Information Technology Act, 2000
48. Section 2(1)(o) of Information Technology Act, 2000
49. Peter Carey, "Data Protection: A Practical Guide to UK and EU Law", 23 (2d ed. 2004)
50. Sagarika Ghose, "Controversy Of Love And Libel", at http://www.outlookindia.com/article.aspx?200468
51. R. Rajagopal v. State of Tamil Nadu, (1994) 6 S.C.C. 632, 639
52. Ian J. Turnbull, "Privacy in the Workplace", CCH Canadian Limited, 2009, 2nd ed. at 93
53. Section 2(1)(o) of Information Technology Act, 2000, "representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;"
54. Organisation for Economic Co-Operation and Development, Data Protection, Glossary of Statistical Terms, http://stats.oecd.org/glossary/detail.asp?ID=%206903
55. Article 12, Universal Declaration of Human Rights, 1948 at http://www.ohchr.org/EN/UDHR/Documents/UDHR Translations/eng.pdf
56. Section 66 of Information Technology Act, 2000
57. Section 65 of Information Technology Act, 2000
58. Section 72 of Information Technology Act, 2000
59. "Compensation to failure to protect Data", Information Technology (Amendment) Act, 2008
60. Section 43A .Cl.(iii) of Information Technology Act, 2000
61. "downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;"
62. Section 43of Information Technology Act, 2000

63. Section 43A of Information Technology Act, 2000
64. "Penalty for damage to computer, computer system, etc" Information Technology Act, 2000
65. Section 43A of Information Technology Act, 2000
66. Section 43A of Information Technology Act, 2000
67. "Punishment for Disclosure of Information in Breach of Lawful Contract", Information Technology (Amendment) Act, 2008
68. Section 2(1) (k) of Information Technology Act, 2000
69. "Tampering with computer source documents", Information Technology Act, 2000
70. "Hacking with computer system.", Information Technology Act, 2000
71. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
72. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
73. NASSCOM Announces Milestones for Its 'Trusted Sourcing' Initiative, NASSCOM
74. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
75. DSCI Excellence Awards 2011 at http://www.dsci.in/sites/default/files/PR_DSCI%20Excellence%20Awards_post.pdf on 22/07/2011
76. Anoop Narayanan, "Protection of personal data", The Economic Times at http://articles.economictimes.indiatimes.com/2007-01-29/news/27669329_1_privacy-personal-information-icici-bank (Last seen on 29/01/2007)
77. Vakul Sharma, " White Paper on Privacy Protection in India", at http://www.iamai.in/Upload/IStandard/White%20Paper%20on%20Privacy.%202007.pdf , http://www.majmudarindia.com,
78. Ms. M. Shanthi, "News on Right to Information" at www.rti.org.in
79. Section 73of Indian Contract Act, 1872
80. Subhajit Basu, "Policy-Making, Technology And Privacy In India", The Indian Journal Of Law And Technology, Volume 6, 2010 at http://www.ijlt.in/archive/volume6/3.pdf
81. CRID,"First Analysis of the Personal Data protection Law in India",University of Namur at http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_india_en.pdf
82. CRID,"First Analysis of the Personal Data protection Law in India",University of Namur at http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_india_en.pdf
83. CRID,"First Analysis of the Personal Data protection Law in India",University of Namur at http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_india_en.pdf
84. Following is the provisions dealing with confidentiality in the employment contract of a leading Indian IT Company WIPRO:
    "In consideration of the opportunities training and access to new technologies and know how that will be made to you, you will be required to comply with the confidentiality policy of the company. Therefore please ensure that you maintain as secret and confidential all Confidential Information (as defined from time to time in the confidentiality policy of the company) and shall not use or divulge or disclose any such Confidential Information except as may be required under obligation of law or as may be required by WIPRO and in the course of your employment. The covenant shall endure during your employment and for a period of one year from the cessation of your employment with WIPRO (irrespective of the circumstances of, or the reasons for, the cessation) In your work for WIPRO, you will be expected not to use or disclose any confidential information, including trade secrets, of any former employer or other person with whom you have an obligation of confidentiality and by signing below you affirm that you have no conflicting obligations or non-compete agreements that would prevent you from working without limitation for WIPRO Technologies"
85. Rodney D. Ryder & Ashwin Madhavan,, "Data Protection, Privacy and Corporate Compliance: The Law and Emerging Trends in India" at http://information5.com/d/data-protection,-privacy-and-corporate-compliance-the-law-and-w3109.html
86. Rodney D. Ryder & Ashwin Madhavan, "Data Protection, Privacy and Corporate Compliance: The Law and Emerging Trends in India",at http://information5.com/d/data-protection,-privacy-and-corporate-compliance-the-law-and-w3109.html
87. Rodney D. Ryder & Ashwin Madhavan, "Data Protection, Privacy and Corporate Compliance: The Law and Emerging Trends in India", at http://information5.com/d/data-protection,-privacy-and-corporate-compliance-the-law-and-w3109.html
88. Section 63B of the Indian Copyright Act of 1957
89. Burlington Home Shopping v. Rajnish Chibber 61 (1995) DLT 6
90. Section 2(o) of the Indian Copyright Act of 1957
91. Umesh Pandit, "Intellectual Property Rights in India", knol Beta, at http://knol.google.com/k/umeshpandit/intellectual-property-rights-in-india/r0tyv5xaaisc/45#
92. Manisha Singh, "India's Patent law - is it TRIPs compliant?" (2005) at http://www.managingip.com/article/1321451/Indias-patent-lawis-it-TRIPs-compliant.html.
93. Eastern Book Company v. D.B. Modak [Appeal (Civil) 6472 of 2004]

94. AIR 1955 Mad 391
95. Vinita Bali, "Data Privacy, Data Piracy: Can India Provide Adequate Protection for Electronically Transferred Data?" , Santa Clara University School of Law, Oct. 2006
96. Section 403of India Penal Code
97. Section 22 of Indian Penal Code
98. Manisha Singh, "India's Patent law - is it TRIPs compliant?" (2005) at http://www.managingip.com/article/1321451/Indias-patent-lawis-it-TRIPs-compliant.html
99. Section 405 of Indian Penal Code
100. Section 424 of Indian Penal Code
101. Section 420 of Indian Penal Code
102. Section 23 of Indian Penal Code
103. Section 425of Indian Penal Code
104. Ministry of Personnel, Public Grievances & Pensions, Right to Privacy Bill, 2011
105. Section 78 of the Privacy Bill, 2011
106. Section 5(2) of the Indian Telegraph Act, 1885
107. (2011) 7 SCC 69
108. Section 6(2) of Right to Privacy Bill, 2011
109. Section 2(n) of Information Technology Act, 2000
110. Section 48 of Information Technology Act, 2000
111. Indian Telegraph (Amendment) Rules, 2004 at www.dot.gov.in/Acts/rules.doc
112. Prevention of Terrorism Act, 2002 at www.satp.org/satporgtp/countries/india/document/actandordinances/POTA.htm
113. Right to Information Bill, 2004 at www.humanrightsinitiative.org/programs/ai/rti/india/national/rti_bill_2004_tabled_version.pdf