The John Marshall Journal of Information Technology & Privacy Law

Volume 27
Issue 4 *Journal of Computer & Information Law - Summer 2010*

Article 1

Summer 2010

How Safe is this Shore? - Data Protection and BPOs in India, 27 J. Marshall J. Computer & Info. L. 539 (2010)

Kritika Bharadwaj

ARTICLES

HOW SAFE IS THIS SHORE? - DATA PROTECTION AND BPOS IN INDIA

KRITIKA BHARADWAJ*

INTRODUCTION

"There is so much fog in the windshield and I don't think anybody has a crystal ball."[1]

—N. R. Narayana Murthy[2]

The fading of international trade barriers and the development in telecommunication and Information Technology ("IT") capability over the past decade has given rise to a boundary-less world, where organizations across the world are increasingly inter-linked with one another. This has paved way for an intense global competition, with a fight to ease costs in order to meet the needs of the global market. Enter the ITeS/BPO industry.

India has one of the fastest growing demographics of personal computer and Internet usage,[3] following the United States of America ("U.S.") and the United Kingdom ("U.K."). In the light of this progress, there is no doubt that India has benefited from the worldwide process of outsourcing. On the same note, the service offered by India has rendered her indispensible to countries around the world, including the U.S. and the U.K. However, where convenience, speed, and accessibility are taken for granted in this digital era, this paradigm shift has consequently re-

* B.A.L., LL.B, Bangalore University and PGDIPR, National Law School of India University, Karnataka, India.

1. *Infosys Profits Beat Forecasts*, BBC NEWS, Oct. 10, 2001, http://news.bbc.co.uk/2/hi/business/1591522.stm.

2. *Id.* N. R. Narayana Murthy is the Chairman and Chief Executive Officer of Infosys, the second largest software exporter in India.

3. Nipul Patel & Susan E. Conners, *Outsourcing: Data Security and Privacy Issues in India*, ISSUES IN INFO. SYS. 14 (2008), *available at* http://iacis.org/iis/2008_iis/pdf/S2008_888.pdf.

sulted in changes in its management and control, safeguard measures, and a surge of unprecedented threats and liabilities. The phenomenon of business processes has also "brought in its wake some unforeseen challenges in the area of data security and privacy."[4] At present the legal framework on data protection is in a nascent stage and is scattered over a broad spectrum of laws. The Information Technology Act of 2000 ("IT Act 2000"), intellectual property rights laws, contractual laws, and company policies aligned with the international specifications govern the protection of data in the Indian Business Process Outsourcing ("BPO") industry.

Striving to match clients' needs and processes is no longer sufficient to keep up with the constantly rising pace of the BPO industry's development. It is innovation and the ability to improve and secure the existing systems and models that will keep India ahead of the competition. Given that India has always welcomed change and development in the technological arena, the question that seeks an answer is whether India is as progressive in updating laws so as to keep pace with technological and industrial development.

1. UNDERSTANDING DATA PROTECTION

1.1 Meaning of Data Protection

"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 personal data."[5] It is the legal safeguard used to prevent misuse of information stored in computers - particularly information about individual people. Data protection encompasses control and management of the data creation and creation of basic rights and obligations and also stipulates penalties and remedies in case of misuse of the data.

Etymologically, the word "data" means "something given."[6] The term "data" has been defined under section 2(o) of the IT Act of 2000[7] as:

---

4. *Data Security Council of India (DSCI): A Self Regulatory Initiative in Data Security and Privacy Protection*, NASSCOM, http://www.nasscom.in/Nasscom/templates/NormalPage.aspx?id=51973 (last updated Dec. 4, 2008).

5. Organisation for Economic Co-Operation and Development, *Data Protection*, Glossary of Statistical Terms, Nov. 9, 2005, http://stats.oecd.org/glossary/detail.asp?ID=6903.

6. *Data*, Wikipedia, http://en.wikipedia.org/wiki/Data (last modified Oct. 17, 2010).

7. Information Technology Act, No. 21 of 2000, India Code. The Act is often presented in India as the text regulating data protection under Indian Law. The aim of the IT Act was to set up India's first ever information technology legislation. This Act is based on the Model Law on Electronic Commerce Adopted by the United Nations Commission on International Trade Law (UNCITRAL), a United Nations General Assembly Resolution. *See*

> a 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.[8]

Data is the "physical representation of information in a manner suitable for communication, interpretation, or processing by human beings or by automatic means."[9] The definition of "data" and its protection in the Indian context, does not give a comprehensive understanding of the term.

Prior to the enactment of the Constitution of India in 1950, there was no guarantee of privacy rights for the citizens of India. Common Law addressed the right of privacy under certain criminal and tort laws.[10] Protection of data was, however, unheard of at the time. The scope of this protection was limited to the person and the property of a person and each of the terms were used in a narrow sense. After the Constitution of India was enacted, the fundamental right to privacy was not expressly guaranteed; however, the judiciary interpreted privacy rights to be considered as fundamental rights.[11]

With the development of technology and the computerization of governmental and other regulatory agencies, there was a shift of concern to privacy of collected and stored data. The IT Act of 2000 was enacted to

---

G.A. Res. 51/162, U.N. Doc. A/Res/51/162 (Jan. 30, 1997), *available at* http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N97/763/57/PDF/N9776357.pdf?OpenElement.

8. The Information Technology Act, No. 21 of 2000, INDIA CODE, section 2(o).

9. UNITED NATIONS STATISTICAL COMMISSION AND ECONOMIC COMMISSION FOR EUROPE, CONFERENCE OF EUROPEAN STATISTICIANS STATISTICAL STANDARDS AND STUDIES No. 53 at 6 (2000), *available at* http://www.unece.org/stats/publications/53metadaterminology.pdf; THE OXFORD DICTIONARY OF STATISTICAL TERMS (Yadolah Dodge ed., Oxford University Press, 2003).

10. CRID UNIVERSITY OF NAMUR, FIRST ANALYSIS OF THE PERSONAL DATA PROTECTION LAW IN INDIA (2005), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/final_report_india_en.pdf ("The criminal law protected the person, property and dwelling house and punished imputation of un-chastity to a female. The law of torts was reputed as providing an additional dimension of protection of individual interests in reputation as also the person and property with an admonition that the least touching of another in anger was assault actionable in damages").

11. The Supreme Court of India has held that right in the Right to Life and Personal Liberty enshrined in Article 21 of the Constitution, through an extensive interpretation of the phrase "Personal Liberty" includes the right to privacy of the individual. *See e.g.*, Kharak Singh v. State of Uttar Pradesh, A.I.R. 1963 S.C. 1295; People's Union for Civil Liberties v. Union of India, (1997) 1 S.C.C. 301; R. Rajagopal v. State of Tamil Nadu, A.I.R. 1995 S.C. 264; *See also* Neetika Yadav & T. Priyadarshini, *Adequately Protected in India: The Need for a Separate Legislation*, MAINSTREAM WEEKLY, (July 12, 2008), http://www.mainstreamweekly.net/article818.html.

cope, generally, with e-commerce. Banks and medical institutions recognized the need and obligation to keep certain information confidential. Although no specific statutes were enacted to provide explicit provisions imposing a secrecy obligation, the awareness and practice of the same was accelerated.

Around the year 2003, the Indian government intended to enact a comprehensive data protection law, so as to give impetus to the flow of personal information from the European Union ("E.U.") into India. The National Association of Software and Service Companies ("NASSCOM") and the Indian Ministry of Information Technology drafted a statute modeled after the E.U. Directive.[12] However, this move turned out to be a failure. The Indian government, industry associations, and legal experts agreed to revise the IT Act of 2000, or to draft an agreement similar to the Safe Harbor Principles, contracted between the E.U. and the U.S.[13]

Not only has the term "data" evolved with time, but the means of protecting data have also undergone considerable change. Although India does not have a specific law regarding data protection, steps are being taken to safeguard and manage data.

1.2 Need for Data Protection

Awareness about data protection and the growing need for the same is of pragmatic importance in this day and age of a digitized environment. The contrast in the awareness and sensitivity to the issue is blatant in the very fact that privacy in the West is synonymous to information privacy, financial information and identity theft, whereas among the Indian subjects, privacy is primarily associated with personal space and subjects.[14]

The protection of data, arising from the precincts of individual privacy obliges that the individual must be in a position to exercise control

12. *See* Directive 95/46/EC of the European Parliament and of the Council of 24 Oct. 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, Official Journal of the European Community, No.L281/31 (Nov. 23, 1995), *available at* http://www.privacycommission.be/en/static/pdf/wetgeving/directive-95-46-en.pdf.

13. David Bender, *Data Protection Law in India: A Change in Direction,* Privacy and Security Law Report (Jan. 12 2004), *available at* http://www.whitecase.com/publications/detail.aspx?publication=346.

14. P. Kumaraguru & L. Cranor, *Privacy Perceptions in India and the United States: An Interview Study*, (Aug. 5, 2009), *available at* http://www.cs.cmu.edu/~ponguru/tprc_2005_pk_lc_en.pdf. "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." *Id.* at 6.

over the data and its management. A specific framework of law is, therefore, required to create basic rights and duties and provide for remedies.

The advent of digitized and computerized systems, which makes it easy to store and disseminate information via automated processes, has made privacy related to the protection of personal data an issue of growing concern in progressive nations.[15] The storage of works in digital form in an electronic medium, the extensive use of the Internet, and new trends in downloading and copying, have increased the need for better protection of data.

1.3 Current Position of Data Protection in India

In India, the protection of privacy, a basic human right recognized by the Universal Declaration of Human Rights of 1948,[16] was derived from common law torts and constitutional law.[17] A person may be held tortiously liable for unlawful invasion of privacy of another,[18] whereas under constitutional law, this right has been implicitly recognized,[19] but is subject to reasonable State-imposed restrictions. However, the IT Act of 2000 is considered to be the most widely recognized legislation that covers data protection.[20] In order to cover the shortcoming in the IT Act of 2000, contractual clauses that the Indian companies have agreed to come into play in the trade with overseas clients.[21]

1.3.1 *Constitutional Law*

The protection of data finds its roots in the individual's right to privacy.[22] In a number of decisions, the Supreme Court of India has upheld

15. Peter Carey, Data Protection: A Practical Guide to UK and EU Law (Oxford: OUP, 2nd ed., 2004).

16. Universal Declaration of Human Rights, G.A. Res. 217 A (III), U.N. Doc. A/RES/217 (III), Article 12 (Dec. 10 1948), *available at* http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf.

17. 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.

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

19. India Const. art. 21.

20. Press Release, *NASSCOM Announces Milestones for Its 'Trusted Sourcing' Initiative*, NASSCOM (Apr. 23 2007), http://www.nasscom.in/Nasscom/templates/NormalPage.aspx?id=51330.

21. Vakul Sharma, *Legal Issues for Data Protection: Myths and Realities* (Feb., 17, 2009).

22. Carey, *supra* note 15. The right to confidential information arises under privacy law (personal information relating to individuals) or trade secrets law (relating to commercial and scientific information). Raymond T. Nimmer, Information Law 1 (West Group, 2002).

the right to privacy[23] as a fundamental right.[24] Moreover, Article 300A of the Constitution of India, provides for the right to property as a constitutional right.[25] This makes intellectual property in the data a subject of this right.[26]

To adhere to the international human rights instruments (International Covenant on Civil and Political Rights,[27] International Covenant on Economic Social Cultural Rights,[28] and Universal Declaration of Human Rights[29]), the Indian Parliament has enacted a variety of legislation to safeguard recognized human rights.[30] For example, the Protection for Human Rights Act of 1993 provides for the constitution of a National and State Human Rights Commission and Human Rights Courts for better protection of Human Rights and for connected or incidental matters.[31]

---

23. Privacy is an individual's claim to control access to or use of personal information. U.S. DEP'T OF COMMERCE, PRIVACY AND THE NII: SAFEGUARDING TELECOMMUNICATION-RELATED PERSONAL INFORMATION 5 (1995), *available at* http://www.ntia.doc.gov/ntiahome/provwhitepaper.html.

24. Kharak Singh v. State of Uttar Pradesh, A.I.R. 1963 S.C. 1295; R. Rajagopal v. State of Tamil Nadu, (1994) 6 S.C.C. 632; Gobind v. State of Madhya Pradesh, (1975) 2 S.C.C. 148; Bender, *supra* note 13.

25. INDIA CONST. art. 300A.

26. The United States Supreme Court has held, "a business, in making unauthorized disclosures, it was deprived of its right to exclusive use of the information, for, exclusivity is an important aspect of confidential information and the most private property for that matter." Carpenter v. United States, 484 U.S. 19, 26-27 (1987).

27. International Covenant on Civil and Political Rights, G.A. Res. 2200A (XXI), 21 U.N. GAOR, 23 March, 1976, Supp. No. 16 at 52, U.N. Doc. A/6316 (1966), 999 U.N.T.S. 171.

28. International Covenant on Economic, Social and Cultural Rights, G.A. Res. 2200A (XXI), 21 U.N.GAOR, 3 January, 1976, Supp. No. 16 at 49, U.N. Doc. A/6316 (1966), 993 U.N.T.S. 3.

29. Universal Declaration of Human Rights, G.A. Res. 217 A (III), U.N. Doc. A/RES/217 (III), Article 12 (Dec. 10 1948), *available at* http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf.

30. These include, *inter alia*, The Commission of Sati (Prevention) Act, No. 3 of 1987, INDIA CODE; The National Commission for Minorities Act, No. 19 of 1992, INDIA CODE; The Protection of Civil Rights Act, No. 22 of 1955, INDIA CODE; The National Commission for Women Act, No. 20 of 1990, INDIA CODE; The National Commission for Backward Classes Act, No. 27 of 1993, INDIA CODE; Dowry Prohibition Act, No. 28 of 1961, INDIA CODE; The Scheduled Castes and the Scheduled Tribes (Prevention of Atrocities) Act, No. 33 of 1989, INDIA CODE; The Juvenile Justice Act, No. 53 of 1986, INDIA CODE; The Child Labour (Prohibition and Regulation) Act, No. 61 of 1986, INDIA CODE.

31. Protection for Human Rights Act, No. 10 of 1993, INDIA CODE (defining human rights "the rights relating to life, liberty, equality and dignity of the individual guaranteed by the Constitution or embodied in the International Covenants and enforceable by courts in India").

1.3.2 *Information Technology Act of 2000*

The IT Act of 2000 is considered to be the law that governs data and its protection.[32] When the IT Act of 2000 was passed, the concept of "data protection" was not envisaged. The only safeguard that the IT Act of 2000 provides to data is with respect to the penalty in a case of breach or unlawful activity. The provision under the IT Act of 2000 that deals with unauthorized access and damage to data is Section 43.[33] Section 43(b) affords cursory safeguards against breaches in data protection.[34] The scope of Section 43(b) is limited to the unauthorized access, downloading, copying, extraction, or damage of data from a computer system.[35] However, the Information Technology (Amendment) Act of 2008 ("IT Act of 2008")[36] has removed any cap on the amount of damages.[37] The damages under Section 43 were quantified at Rupees one

32. Information Technology Act, No. 21 of 2000, INDIA CODE, Section 1(2) ("it shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention thereunder committed outside India by any person").

33. Information Technology Act, No. 21 of 2000, INDIA CODE, Section 43:

> Penalty for damage to computer, computer system, etc.
> If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, -
> (a)(i) accesses or secures access to such computer, computer system or computer network;
> (b)(ii) downloads, copies or extracts any data, computer database or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
> (c)(iii) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
> (d)(iv) damages or causes to be damaged and computer, computer system or computer network, data, computer database or any other programme residing in such computer, computer system or computer network;
> (e)(v) disrupts or causes disruption of any computer, computer system or computer network;
> (f)(vi) denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;
> (g)(vii) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of the IT Act 2000 rules or regulations made there-under;
> (h)(viii) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system or compute network, he shall be liable to pay damages by way of compensation not exceeding Rupees one crore to the person so affected.

34. Information Technology Act, No. 21 of 2000, INDIA CODE, Section 43(b); *see also* Information Technology Act, No. 21 of 2000, INDIA CODE, Section 43(h)43 ("he shall be liable to pay damages by way of compensation not exceeding Rupees one crore to the person so affected").

35. Information Technology Act, No. 21 of 2000, INDIA CODE, Section 43 ("unauthorized access, downloading, copying, extraction or damages of data from a computer system are the only offenses punishable by fine of up to one crore").

36. Information Technology (Amendment) Act, 2008, No. 10, Acts of Parliament, Section 43-A, 2009 (India).

37. *Id.*

crore, but the IT Act of 2008 has removed this limit of one crore and made the damages unliquidated; thus, the damages that one can suffer under these instances can be well above Rupees one crore.[38] The IT Act of 2000 affords various criminal penalties or a monetary penalty in cases of hacking[39] and intentional destruction, alteration of personal data, or concealment of computer source code.[40]

Section 43-A of the IT Act of 2008 deals with compensation for failure to protect data by a corporation involved in "possessing, dealing, or handling any sensitive personal data or information in a computer resource which it owns, controls, or operates" and "causes wrongful loss or wrongful gain to any person."[41] In order to ensure that a corporation is liable under this section, it has to be proved that the corporation was negligent in implementing "reasonable security practices and procedures."[42] This section places liability on an intermediary as well.[43] However, the liability of an intermediary sued under section 43-A is diluted in section 79 of the Act, which inserts both "knowledge" and "best efforts" as qualifiers prior to assessing penalties.[44] Moreover, section 85

---

38. *Id.*

39. Information Technology Act, No. 21 of 2000, INDIA CODE, Section 66:

Hacking with Computer System –

(1) Whoever with the intent of cause or knowing that is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking,

(2) Whoever commits hacking shall be punished.

40. Information Technology Act, No. 21 of 2000, INDIA CODE, Section 65:

Tampering with computer source documents –

Whoever knowingly or intentionally conceals, destroy, or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punished with.

41. Information Technology (Amendment) Act, 2008, No. 10, Acts of Parliament, Section 43-A, 2009 (India).

42. *Id.*:

Compensation for failure to protect data –

Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

43. *Id.*

44. Information Technology Act, No. 21 of 2000, INDIA CODE, Section 79:

Network service providers not to be liable in certain cases

For the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this Act, rules or regulations made thereunder for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence for contravention.

of the IT Act of 2008 also invokes entity liability, limited to the specified illegal acts of persons for intentional or negligent acts that result in a breach of the specific violations under the IT Act of 2000.

The IT Act of 2000, under section 72, prohibits breach of confidentiality and privacy, penalizing an individual who commits a breach in the exercise of the powers granted, without the consent of the concerned individual.[45] It may be said that this is the only section of the IT Act of 2000 that may be extended to data in all its forms, electronic as well as non-electronic.[46] There is also a provision for criminal liability in cases of disclosure of information in breach of lawful contracts, under the penal provisions of section 72-A of the IT Act of 2008, with an intention to cause wrongful loss or gain[47] and without the consent of the person whose personal information is being disclosed.[48] The Central Government established a special tribunal, the Cyber Appellate Tribunal, and all matters arising out of the IT Act of 2000 are within this tribunal's jurisdiction.[49]

1.3.3 *Intellectual Property Rights Laws*

Computer software (including computer programs,[50] databases, computer files, preparatory design material, and associated printed doc-

45. Information Technology Act, No. 21 of 2000, INDIA CODE, Section 72.

46. *Id.*:

> Breach of confidentiality and privacy:
> Save as otherwise provided in this Act or any other law for the time being in force, if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

47. INDIAN PENAL CODE, Section 23 (1860) ("'Wrongful Gain' is gain by unlawful means of property which the person gaining is not legally entitled") ("'Wrongful Loss' is the loss by unlawful means of property to which the person losing it is legally entitled").

48. Information Technology (Amendment) Act, 2008, No. 10, Acts of Parliament, Section 72-A:

> Punishment for disclosure of information in breach of lawful contract –
> Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both.'

49. Information Technology Act, No. 21 of 2000, INDIA CODE, Section 48.

50. Section 63B of the Indian Copyright Act of 1957 provides a penalty for any person who knowingly makes use on a computer of an infringing copy of computer program. Indian Copyright Act, No. 14 of 1957, INDIA CODE, Section 63B.

umentation, such as users' manuals) receives copyright protection under Indian laws.[51] The Indian Copyright Act of 1957 "prescribes mandatory punishment for piracy of copyrighted matter commensurate with the gravity of the offense."[52] Computer programs are not *per se* patentable, being patentable only in combination with hardware.[53] Thus in India, by past practice and under current laws, copyright is the preferred mode of protection for computer software.

1.3.4 *Criminal Laws*

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."[54] 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."[55] Therefore, "[a]lthough no jurisprudence has been developed on this interpretation, arguably, movable property encompasses computer-related data and intellectual property."[56] 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.[57] Further, the IPC imposes criminal liability for dishonest or fraudulent concealment or removal of property,[58] and also for when a person "cheats and thereby dishonestly induces the person" in

51. Under section 2(o) of the Indian Copyright Act of 1957, "literary work" includes computer programme, tables and compilations including computer literary databases. Indian Copyright Act, No. 14 of 1957, INDIA CODE Section 2(o).

52. Umesh Pandit, *Intellectual Property Rights in India*, KNOL BETA, http://knol.google.com/k/umesh-pandit/intellectual-property-rights-in-india/r0tyv5xaaisc/45# (last visited Sept. 22, 2010). *See also* Information Technology Act, No. 21 of 2000 Section 63B.

53. Manisha Singh, *India's Patent law – is it TRIPs compliant?*, MANAGING INTELL. PROP., (2005) *available at* http://www.managingip.com/article/1321451/Indias-patent-lawis-it-TRIPs-compliant.html.

54. Vinita Bali, *Data Privacy, Data Piracy: Can India Provide Adequate Protection for Electronically Transferred Data?* (Legal Studies Research Papers Series, Social Science Research Electronic Paper Collection, Santa Clara University School of Law, Working Paper No. 06-10, Oct. 2006), *available at* http://law.bepress.com/cgi/viewcontent.cgi?article=7349&context=expresso; INDIA PENAL CODE, Section 403 (1860).

55. INDIA PENAL CODE, Section 403 (1860).

56. Bali, *supra* 54. Singh, *supra* note 53; INDIA PENAL CODE, Section 22 (1860) (defining "movable property" as "corporeal property of every description, except land and things attached to the earth or permanently fastened to anything which is attached to the earth.").

57. INDIA PENAL CODE, Section 405 (1860). Liability extends to employees and agents of the violator, and the crime is punishable by imprisonment and/or fine. *Id.*

58. *See* INDIA PENAL CODE, Section 424 (1860) ("Whoever dishonestly or fraudulently conceals or removes any property of himself or any other person, or dishonestly or fraudulently assists in the concealment or removal thereof, . . . shall be punished").

possession of the property to deliver the said property.[59] Furthermore, section 425 imposes liability on a third party who intends to cause wrongful loss or damage to the property of another person, whether or not the person is the owner of the property.[60]

1.3.5 *Contractual Obligations*

Non-E.U. states where data protection has not been found to be "adequate,"[61] such as in India,[62] rely on an alternative avenue and *ad hoc* solutions to procure and continue business transactions. The European Commission and the Data Protection Commissioner have the power to endorse "model contracts" specific to the transferring countries' circumstances, as well as the power to approve particular contracts or other arrangements that provide satisfactory safeguards.[63] Data Exporters in other countries enter into a contract with an Indian BPO detailing the specific duties and obligations of both parties involved. Therefore, in the absence of legislation that offers sufficient and adequate legal protection for personal data, any uncertainty regarding doing business with an Indian BPO is a matter of negotiation of the relevant contract using appro-

---

59. *See* INDIA PENAL CODE, Section 420 (1860) ("Whoever cheats and thereby dishonestly induces the person deceived any property to any person, or to make, alter or destroy the whole or any part of a valuable security, or anything which is signed or sealed, and which is capable of being converted into a valuable security, shall be punished").

60. *See* INDIA PENAL CODE, Section 425 (1860) ("Whoever with intent to cause, or knowing that he is likely to cause, wrongful loss or damage to the public or to any person, cause the destruction of any property, or any such change in any property or in the situation thereof as destroys or diminishes its value or utility, or affects it injuriously, commits 'mischief'. . ..It is not essential to the offence of mischief that the offender should intend to cause loss or damage to the owner of the property injured or destroyed").

61. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data 95/46/EC, 1995 O.J. (L 281), *available at* http://www.privacycommission.be/en/static/pdf/wetgeving/directive-95-46-en.pdf.

62. *Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries*, EUROPEAN COMMISSION, http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm (last updated Aug. 6 2010).

63. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data 95/46/EC, 1995 O.J. (L 281), *available at* http://www.privacycommission.be/en/static/pdf/wetgeving/directive-95-46-en.pdf; EUROPEAN COMMISSION, FIRST ORIENTATIONS ON TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES – POSSIBLE WAYS FORWARD IN ASSESSING ADEQUACY, (June 26 1997), *available at* http://webcache.googleusercontent.com/search?q=cache:eXf1aJhhuOoJ:ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1997/wp4_en.pdf+site:ec.europa.eu+Report+of+the+EUROPEAN+COMMISSION+WORKING+PARTY+ON+THE+PROTECTION+OF+INDIVIDUALS+WITH+REGARD+TO+THE+PROCESSING+OF+PERSONAL+DATA,+Free+Movement+of+Information+and+Data+Protection,+including+international+aspects,+1997+final&hl=en&gl=in.

priate legal expertise and advice. Apart from contractual obligations with the Data Exporters, the employment contracts between the BPO and its employees also specify that the employees have to maintain confidentiality regarding all such information that they may process.[64]

1.3.6 *The Credit Information Companies (Regulation) Act of 2005*

The Credit Information Companies (Regulation) Act of 2005 "imposes duties on credit information companies, credit institutions, and specified users while processing credit data."[65] Additionally, the Reserve Bank of India has the authority to penalize any credit information company, credit institution, or specified user, for violating this Act.[66] On this ground, the "Reserve Bank of India could be considered as a specific data protection authority in the field of credit information."[67]

1.4 Shortcomings in the Provisions for Data Protection

Although India has been proactive in making provisions for the protection of data, it has a long way to go in order to reach the heights of protection afforded by international provisions for data protection in foreign countries. The protection of data in India needs to be critically examined and the lacuna must be spotted. Only then can a measure for its elimination be taken. The shortcomings in the national data protection laws may be examined as follows.

1.4.1 *Information Technology Act of 2000*

The major shortcoming in the IT Act of 2000, as amended by the IT Act of 2008, is that none of the three objectives detailed in the preamble[68] recognize the protection and preservation of data. The very fact that data protection is outside the scope and purpose of the IT Act weakens the relevance of its provisions. Moreover, "data" under the IT Act of

---

64. Rodney D. Ryder & Ashwin Madhavan, *Data Protection, Privacy and Corporate Compliance: The Law and Emerging Trends in India*, Scribboard (Apr. 18, 2009), http://www.scribboard.com/whitepapers/data_privacy.pdf.

65. *Id.*; CRID University of Namur, *supra* note 10, at 49.

66. *Id.*

67. *Id.*

68. Information Technology Act, No. 21 of 2000, India Code:

> An Act to provide legal recognition for transactions carried out by means of electronic date interchange and other means of electronic communication, commonly referred to as "electronic commerce," which involve the use of alternative to paper-based methods of communication and storage of information to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, 1860, the India Evidence Act, 1872, the Banker's Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.

2000 is restricted to data stored and processed in the electronic form.[69] Considering that India still employs conventional methods of data storage, transfer, and process, all forms of data other than electronic data are susceptible to unauthorized use that might adversely affect the subjects of such data. Therefore, this legislation does not provide protection to data stored in the non-electronic medium.

Section 43 penalizes any unauthorized access to a computer, computer system or computer network and any unauthorized download, copying or extraction of any data.[70] An interpretation of section 43 shows that it provides for protection of data in a very limited sense - it is only a punitive provision.[71] The IT Act of 2000 penalizes any individual who misuses electronic data, without the permission of the owner or any other person in charge of such data. This penalty is inadequate because it does not address the concern of misuse of data by the person responsible for such data. Section 43 does not address data protection. Rather, it is merely recourse to compensate the individual for any damage resulting from unauthorized access or damage to data.

"Data protection" in its entirety means the collection, retention, protection and proper disposal of the data collected.[72] Therefore, section 43 of the IT Act of 2000 is very limited because it only provides a remedy for unauthorized access or damage to stored data. It does not address many of the principles provided in the Data Protection Act of 1998 ("DPA").

In the provisions under the DPA in the U.K., personal information and sensitive personal information have different levels of protection, where loss, unauthorized access or disclosure of sensitive personal information is considered to have a deeper impact on the data subject.[73] In contrast to the DPA, the IT Act of 2000 does not assign a higher level of care or protection to sensitive personal information. In essence, there is

---

69. Information Technology Act, No. 21 of 2000, INDIA CODE, Section 2(o):

"data" means a 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.

In contrast, the DPA recognizes and protects data stored in any electronic medium or a relevant filing system (such as a salesperson's diary). Data Protection Act, 1998, Section 1 (Eng.).

70. Information Technology Act, No. 21 of 2000, INDIA CODE, Section 43.

71. *Id*.

72. *Id*.

73. Data Protection Act, 1998 (Eng.). The DPA has defined Personal data and Sensitive personal data under two separate provisions of law. While section 1 deals with Personal data, section 2 defines the scope of Sensitive personal data. The conditions relevant for the purpose of the application of data protection principles are different for personal data and sensitive personal data, as laid down in Schedule 2 and Schedule 3 respectively.

no difference between personal information and sensitive personal information in relation to data protection. Indeed, "personal information" is not defined in judicial precedent or the IT Act of 2008. Because this term has not been defined, it is difficult to give an exact interpretation of the provisions.

Section 43-A of the IT Act of 2008 places liability on a corporate body only if it has been negligent in implementing its security practices and procedures in relation to the data possessed, controlled or handled by it.[74] There is a significant difference between "negligence to implement" and "failure to implement." The former requires the test of reasonableness to be satisfied before there can be any claim of negligence, while the latter requires only non-performance of the required action. Therefore, there is no liability for the corporate body in cases of failure to implement its security practices and procedures, thereby widening their scope for escaping liability.

The terms "wrongful gain" and "wrongful loss" are used under section 43-A of the IT Act of 2008.[75] However, these terms have not been clearly defined with relevance to data protection, either under statutes or any judicial precedents. It is unclear whether these terms derive their meaning from their definition under the substantive penal law of India, the Indian Penal Code of 1860. Therefore, it is difficult to comprehend the true meaning and application of this section in light of these undefined terms.

The section also makes a reference to "reasonable security practices and procedures," which has been defined under the IT Act of 2008.[76] The three methods by which reasonable security practices and procedures can be determined are: 1) by agreement; 2) by law; and 3) by prescription by the Central Government.[77] However, there is no law in India that defines this term and it will be some time before the Central Government promulgates the necessary regulations to give meaning to this term. Until these regulations are created, a corporation is not liable if the corporation does not agree with the person providing the information to define reasonable security practices and procedures, and then proceeds to dis-

74. Information Technology (Amendment) Act, 2008, INDIA CODE, Section 43-A.

75. *Id.*

76. *Id.*

77. Information Technology (Amendment) Act, 2008, INDIA CODE, Section 43-A, Explanation (ii):

> "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

close that information, even if the corporation causes loss or gain to that person. Thus, the protections are meaningless.

Under the IT Act of 2008, section 43-A places liability on an intermediary as well. However, an intermediary sued under section 43-A, can claim immunity under section 79, if the intermediary satisfies the test laid down under section 79.[78] Therefore, although the law creates personal liability for illegal or unauthorized acts, little effort is made to ensure that Internet service providers or network service providers, as well as entities handling data, are responsible for the safe distribution or processing of the data.[79]

Section 72-A clearly requires that a person who discloses personal information, thereby causing wrongful loss or gain, to have done so willfully.[80] Hence, in order to make a person liable it has to be proved that the person disclosing the personal information did so with an intention to cause wrongful loss or gain.[81] Mere proof of the damage is insufficient.[82] Moreover, section 72-A does not help individuals monetarily. It imposes penal consequences on such persons by way of a fine,[83] which is insufficient to compensate the injured party.

Further, section 72-A is restricted to information about individuals and relates only to personal information obtained under service contracts.[84] This section also makes it evident that disclosure of personal information with intent to cause wrongful loss or gain has to be done without the consent of the person, whose personal information is being disclosed.[85] It may be stated that this provision has not been drafted to cover all situations. In many cases, corporations and individuals when entering into service contracts, ensure that they obtain consent of the individuals for any future disclosures. There are also standard form contracts where the clauses cannot be negotiated – the parties must accept all clauses. Hence, if disclosure of information is one of the clauses in such contracts, then any disclosure is deemed to be with the consent of the person concerned. Therefore, if such a corporation obtains the individual's consent at the time of entering into service contracts, the protection provided for under this section does not apply. The "consent" referred to in section 72-A can be easily circumvented by corporations and individuals by means of clever drafting when entering into service contracts.

78. Information Technology (Amendment) Act, 2008, INDIA CODE, Section 79.
79. Bali, *supra* note 54.
80. Information Technology (Amendment) Act, 2008, INDIA CODE, Section 79.
81. *Id.*
82. *Id.*
83. *Id.*
84. *Id.*
85. *Id.*

Under section 72, disclosure of information stored in non-electronic medium has not been specifically excluded.[86] However, because the definition of personal information has not been contemplated under the IT Act of 2008, the difficulty arises when there is an intentional disclosure of personal information and the person accused of disclosure contends that the information is not personal. Therefore, it is difficult to ascertain the application and enforcement of this section. Section 72 is insufficient because the section only applies if the breach is committed by a person who has been conferred certain powers under the Act, rules, or regulations.[87]

The Indian laws do not specify conditions under which data can be collected and used, and its limited scope fails to meet the breadth and depth of protection that the E.U. Directive mandates.[88] The Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data, 1980 promulgated by the OECD are also instructive, demonstrating that a large void exists in India's IT Act of 2000.[89]

Any and all matters arising from the IT Act of 2000 are brought before the Cyber Appellate Tribunal ("Tribunal"), established by the notification of the Central Government.[90] One glaring lacuna in this legislation is that there is no provision regarding extra-territorial jurisdiction of this Tribunal. The jurisdictional issue of accessibility in the context of trans-national data protection has not been duly addressed for cases arising out of violations in India where the victim is a non-resident of India. The injured parties, who are non-residents of India, would have to approach a foreign jurisdiction for adjudication of the dispute, thereby incurring the related expense and inconvenience.[91] Also, a question arises as to whether a breach or damage to data is classified as a criminal or civil offense. In the light of this uncertainty, it is unclear whether the extra-territorial provisions of the IPC apply to the IT Act of 2000.

---

86. Information Technology (Amendment) Act, 2008, INDIA CODE, Section 79.

87. *Id.*

88. Bali, *supra* note 54.

89. *Id.*; ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT, RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANS-BORDER FLOWS OF PERSONAL DATA (Sept. 23, 1980), *available at* http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.
The OECD Guidelines were formulated to address the threat that disparities in national legislations could hamper the free flow of personal data across national borders. It was anticipated that the flow of data would greatly increase with the innovation and spread of computer and communications technology.

90. Information Technology Act, No. 21 of 2000, INDIA CODE, Ch. IX, Section 46, 47, & Ch. X, Sections 48 et seq.

91. Bali, *supra* note 54, at 27 ("The limited parties from whom recourse can be sought, the limited circumstances under which remedy may be established, and the limited nature of the damages is even more bare when the avenues for recourse and compensatory sums are viewed from a perspective of third party nationals").

1.4.2 *Criminal Laws*

The protection provided by criminal laws is not sufficient in the context of data protection. At the time of enactment of the IPC, it was not envisioned that the provisions would be used to provide data protection. Although the IT Act of 2000 and IT Act of 2008 have made amendments to the IPC, there has been no change with regard to the application of the IPC to data protection. The meaning of "movable property" is unclear as to whether it extends to include intellectual property. Moreover, the adequacy of the remedies under India's criminal laws is questionable in a trans-national context.[92] As correctly pointed out, "the cost, delay and inconvenience associated with foreign nationals bringing actions in Indian courts offsets the availability of the recourse."[93]

1.4.3 *Intellectual Property Rights Laws*

On perusal of the Indian Copyright Act of 1956, it is evident that the Act does not afford complete protection to data. The penalties under this Act are inadequate in a trans-national context.[94] Moreover, the backlog of cases in the Indian criminal courts is not only detrimental to the enforcement of copyright laws on the national and international front,[95] but it also prolongs litigation. Further, there would be the question of conflicting rights and jurisdictions, thereby duplicating litigation.[96]

1.4.4 *Contractual Obligations*

It is pertinent to note that although the gap in the laws is sought to be filled through contractual recourse, it may not be very effective in the absence of strict laws backing it up. The major drawback in use of model contracts is that the Indian BPO is subject to the jurisdiction of an E.U. Member State and the data protection authority, and any departure from the standard clauses runs the risk of disapproval of the contract by the data protection authority.

In contracts for the transfer of data, a number of third parties may be involved: first, the data subjects; second, the third parties to whom

92. *Id.* at 29.

93. *Id.*

94. *Id.* at 31.

95. Priti H. Doshi, *Copyright Problems in India Affecting Hollywood and Bollywood*, 26.2 SUFFOLK TRANSNAT'L L. REV. 295 (2003).

96. Chapter XII, Section 62 of the Indian Copyright Act of 1957 offers civil remedies for infringement of the copyright by way of institution of a suit before a competent district court. Indian Copyright Act, No. 14 of 1957, INDIA CODE, Ch. XII, Section 62. The IT Act 2000 also established, under section 48, a Cyber Appellate Tribunal, to the exclusion of civil courts, for adjudicating related matters. Information Technology Act, No. 21 of 2000, INDIA CODE, Section 48. Since it is not clear as to whether the protection of data is covered by the Indian Copyright Act of 1957 or the IT Act of 2000, choice of the remedies is questionable.

the data is to be re-exported by the importer; and last, the data protection authorities. However, in the case of breach of contract, the injured party may only seek a remedy against the contracting party.[97] The injured third party may not have proper recourse against the actual wrong-doer. Moreover, in relations with third parties, dispute resolution clauses in the contract between the BPO and the Data Exporter are likely to be of very limited effect. The determination as to the governing law or the competent adjudicating authority will, therefore, be difficult to impose on the third parties in the event of a dispute.

Moreover, the clause indemnifying any loss caused by a third party could prove to be detrimental to the party indemnifying the loss. The third party causing the loss could escape liability and the party to the contract, dealing with that third party, would be responsible instead. Another shortcoming in the application of contractual laws for protection of data is that some outsourcing agreements include a clause limiting the liability of the party. It contains a cap on the amount or extent of damages for which a party may be liable.[98] While this clause, detailing the liquidated damages, makes assessment of the same easier and excludes interference by the courts, it also requires an accurate pre-estimate of the possible damage, which, if not properly calculated, could result in loss to the injured party.

2. DATA PROTECTION IN BPOS IN INDIA

2.1 Role of Indian BPOs in the Indian Economy

In a world where information technology has become the backbone of businesses worldwide, 'outsourcing' is the process through which one company ("Data Exporter") hands over part of its work to another company ("Indian BPO"), making it responsible for the design and implementation of certain business processes.[99] This is done under the

97. The doctrine of privity of contract entails that a contract may be enforced only by and against those persons who are parties to the contract, i.e. the contract cannot extend beyond the parties and that third parties offering no consideration cannot assert any rights under the contract. The rule laid down in TweddleTweedle v. Atkinson, (1861) 123 E.R. 762 laid down the foundation of the doctrine of "Privity of Contract" which means that a contract is a contract between the parties only and no stranger to the contract can sue even if the contract is avowedly made for his benefit. This principle was reaffirmed in Dunlop Pneumatic Tyre Co. Ltd. v. Selfridge & Co. Ltd., (1915) A.C. 847. The Supreme Court of India has by its decisions in cases including Jamna Das v. Ram Autar, (1911) 30 I.A. 7 and M.C. Chacko v. State of Travancore, A.I.R. 1970 S.C. 504 has extended the doctrine to India. Pollock & Mulla, on Indian Contract Act and Specific Relief Acts (Dr. R.G. Padia ed., 13th ed., India: LexisNexis, Butterworths 2008).

98. Bharath Vagadia, Outsourcing to India: A Legal Handbook 57 (Verlag Berlin Heidelberg: Springer, 2007).

99. Christopher L. Sorey, *The Hidden Risks of Outsourcing: Is Your IP Safe Abroad?*, 1 Am. U. Bus L. Brief 33 (2005), *available at* http://www.wcl.american.edu/blb/01/2sorey.pdf

requirements and specifications of the Data Exporter.[100]

2.1.1 *The Indian BPO Trend: History and Development*

Over 200 years ago, Adam Smith propounded the theory of "competitive advantage"[101] in his book *The Wealth of Nations*.[102] Anchored in this theory of competitive advantage, the concept of outsourcing has evolved as a popular corporate strategy. During the 1990s, the Government of India sought economic reformation by way of globalization, liberalization, and privatization.[103] In 1999, the New Telecom Policy that was introduced to develop India's information technology and telecom infrastructure brought about de-regulation of the telecom industry, thereby opening up national, long distance, and international connectivity to competition and reducing costs.[104] This was "heralded the golden era for the ITeS/BPO industry" which resulted in an increased number of inbound/outbound call centers[105] and data processing centers.[106] It initially started with outsourcing of services and business processes like medical transcription, data processing, medical billing and customer support from the U.S. and Europe to other developing countries.[107] "Some of the earliest players in the Indian outsourcing market were

?rd=1 ("Sending work abroad, once called 'offshoring'. . ..occurs when a company hires a foreign company to perform some business function").

100. *Id.*

101. *See Competitive Advantage*, INVESTORWORDS, http://www.investorwords.com/998/competitive_advantage.html (last visited Oct. 23, 2010) (defining competitive advantage as a "[c]ondition which enables a company to operate in a more efficient or otherwise higher-quality manner than the companies it competes with, and which results in benefits accruing to that company").

102. ADAM SMITH, THE WEALTH OF NATIONS (Andrew Skinner ed., Penguin Classics, 1999) (1776).

103. *The Outsourcing History of India,* OUTSOURCE2INDIA, http://www.outsource2india.com/why_india/articles/outsourcing_history.asp (last visited Oct. 23, 2010) ("Until the year 1994, the Indian telecom sector was under the control of the government. The state-owned units in India enjoyed a monopoly in the market. In the year 1994, the government announced a policy under which the sector was liberalized and private participation was encouraged").

104. *See Economic Survey 2004-2005,* Apr. 14, 2009, http://www.indiabudget.nic.in/es2004-05/chapt2005/chap94.pdf ("After the announcement of New Telecom Policy, 1999, progress in telecom in India has been extremely rapid. The total number of telephones (basic and mobile) rose from 22.8 million in 1999 to 88.6 million at the end of October, 2004. . .. Tele-density rose from just 2.32 in 1999 to 8.2 in October 2004").

105. "Call center" means an entity staffed by personnel who answer telephone calls that, e.g., request assistance with various types of problems (a "help-desk"), or deal with reservations for hotels, airlines, car rentals, etc. Bender, *supra* note 13.

106. OUTSOURCE2INDIA, *supra* note 103.

107. *Id.*

American Express, GE Capital, and British Airways."[108] At present, Indian BPOs have expanded their services to include processing insurance claims, credit card transactions,[109] web sales and marketing, accounting, tax processing, document management, telemarketing, Human Resource services, and biotech research.[110] Thus, from manufacturing of goods in countries providing cheap labor,[111] to adapting to multinational companies' off-shoring requirements, today the outsourcing market[112] has "developed into a broad-based business platform backed by leading Indian IT software and services organizations and other third party service providers."[113]

India is one of the world's largest outsourcing data hubs,[114] an industry that is expanding at an annual rate of nine percent.[115] According to a report by NASSCOM,[116] the IT-BPO industry is a "growth engine" for India's economy and has substantially contributed to its increased GDP and employment. The report states that "BPO is the fastest growing segment of the industry and is estimated to reach 12.8 billion dollars in FY2009, growing at 17.5 percent" and that "direct employment is expected to reach nearly 22.3 million, an additional 226,000 employees,

108. *Id.*; *see also BPO India Chronology*, BPOINDIA, http://www.bpoindia.org/knowledgeBase/india-bpo-chronology.shtml (last visited Oct. 23, 2010).

109. Liz Pulliam Weston, *Your Financial Secrets Are Headed Overseas*, MSN MONEY (Apr. 14, 2009), *available at* http://moneycentral.msn.com/content/Banking/FinancialPrivacy/P90682.asp?Printer; David Lazarus, *Credit Agencies Sending Our Files Abroad*, SAN FRANCISCO CHRONICLE (Nov. 11, 2003), *available at* http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2003/11/07/MNG4Q2SEAM1.DTL.

110. Donna Ghelfi, *The 'Outsourcing Offshore' Conundrum: An Intellectual Property Perspective*, WIPO (Apr. 14, 2009), *available at* http://www.wipo.int/export/sites/www/sme/en/documents/pdf/outsourcing.pdf.

111. A study by the Forrester Research Company estimates that due to such compelling cost-savings, companies will outsource three point three (3.3) million American jobs by 2015. This study also predicted that seventy percent of those jobs would move to India, twenty percent would move to the Philippians, and ten percent to China. John Schwartz, *Experts See Vulnerability as Outsiders Code Software*, N.Y. TIMES, Jan. 6, 2003, § C, at 1.

112. There may be two forms of outsourcing, Information Technology Outsourcing and Business Process Outsourcing. In the former the company offers critical business solutions like desktop management, network and server management, program development, etc., whereas in the latter, the company offers value added services like HR administration, finance and accounting, market research and analysis. BHARATH VAGADIA, OUTSOURCING TO INDIA: A LEGAL HANDBOOK 2 (Verlag Berlin Heidelberg: Springer, 2007).

113. OUTSOURCE2INDIA, *supra* note 103.

114. Michael L. Rustad & Thomas H. Koening, *Extending Learned Hand's Negligence Formula to Information Security Breaches*, 3 I/S: A J. OF LAW & POL'Y FOR INFO. SOC'Y 237 (2007-2008).

115. Jared Sandberg, *It Says Press Any Key, Where's the Any Key?*, WALL ST. J., Feb. 20, 2007, *available at* http://www.uic.edu/classes/ba/ba200w/wang/Indian_call_centers.pdf.

116. NASSCOM*, Executive Summary*, NASSCOM Strategic Review (2009), *available at* http://www.nasscom.in/upload/60452/Executive_summary.pdf.

while indirect job creation is estimated to touch 8 million."[117]

2.1.2 *Importance of Indian BPOs*

The process of outsourcing is "beneficial to both the Data Exporter and the service provider."[118] In this relationship, the service provider allows the outsourcer to lower operating costs and better the quality in certain areas of business, and thereby increase productivity.[119]

NASSCOM cites the following reasons for India's success in the outsourcing industry:

> Abundant, skilled, English-speaking manpower. . .
>
> Fast turnaround times and the ability to offer 24x7 services based on the country's unique geographic location that allows for leveraging time zone differences
>
> Proactive and positive policy environment which encourages ITeS/BPO investments and simplifies rules and procedures.
>
> A friendly tax structure, which places the ITes/BPO industry on par with IT services companies.[120]

Access to a unique combination – "of technically proficient labor force at a relatively cheap cost"[121] - makes India a lucrative option to the foreign companies that are competing with their counter-parts in the market.[122] Moreover, the Indian BPOs have implemented "world-class security standards, to ensure high levels of quality and service delivery."[123] Adherence and compliance with international certification standards and various other data protection regulations ensures the establishment of a proper risk management framework. Moreover, the Data Security Council of India's efforts, "aimed at defining industry standards for data security and privacy," has lead India to develop as a trusted outsourcing destination.[124]

---

117. *Id.*

118. *Outsourcing Industry of India*, DISMAL WORLD http://www.dismalworld.com/world_tour/outsourcing_industry_of_india.php (last visited Oct. 23, 2010).

119. *Id.*

120. *The Outsourcing History of India*, OUTSOURCE2INDIA, http://www.outsource2india.com/why_india/articles/outsourcing_history.asp, (last visited Nov. 11, 2010).

121. Patel & Conners, *supra* note 3.

122. Bender, *supra* note 13 ("In the pertinent job fields, the salaries paid in India are said to be roughly one-eighth of those paid in the United States); Patel & Conners, *supra* note 3.

123. NASSCOM*, Executive Summary*, NASSCOM Strategic Review (2009), *available at* http://www.nasscom.in/upload/60452/Executive_summary.pdf.

124. *Id.*

2.2 Position of Data Protection in BPOs

2.2.1 *Self-regulatory Measures*

In the absence of comprehensive laws regarding data protection in Indian BPOs,[125] the Data Exporters from U.S. and U.K. have implemented various initiatives and security measures in order to satisfy their requirements of data security. These Data Exporters have a rigorous process for selecting the BPO and place "emphasis on data security measures" and identification of and "sharing of best security practices."[126] Security and legal teams are appointed for the purpose of training the employees of the BPO receiving the data.[127] Internal and external auditing of security systems takes place, announced and unannounced, from time to time and some companies deploy their own security consultants to provide protection and ensure security and also conduct and review disaster prevention mock drills.[128] Strict confidentiality and security agreements are entered into prior to awarding any work and transferring any data. The BPOs are required to have dedicated network infrastructures and certifications of compliance with international security standards. During the testing phase, the BPOs have access only to "dummy data."[129] The Data Exporters share production data only when appropriate and necessary, while the testing of production data takes place only on the company network and only at the company location. Masking the sensitive information (social security numbers, names, addresses, etc.) is achieved at the preference of Data Exporter.

The BPOs run a thorough background check of all potential employees, so as to ensure that reliable and trusted persons are employed. "Biometric security devices, including palm and retina scanners, are used to identify employees."[130] In most of the BPOs, "Internet access is limited, unless such access is required for a job function" to guard against "malware and viruses."[131] Further, "[t]ools that can be used to copy data, such as USB drives, mobile phones, cameras or even pens and pencils, are prohibited in the job location"[132] and "[a]ll hardware devices that could be used to store, copy, or forward data are removed from computers."[133]

---

125. Ryder & Madhavan, *supra* note 64.

126. Patel & Conners, *supra* note 3.

127. *Id.*

128. Vir Singh, *Under Pressure India Mulls Step to Protect Privacy*, IEEE Spectrum, Feb. 2005, *available at* http://spectrum.ieee.org/telecom/security/under-pressure-india-mulls-steps-to-protect-privacy.

129. *Id.*

130. *Id.*

131. Patel & Conners, *supra* note 3.

132. *Id*.

133. *Id*.

2.2.2 *NASSCOM Initiatives*

The increasing domestic and global competition and exceeding expectations has forced India to adopt best practices and compliance standards for data security. NASSCOM is India's self-regulatory body for ITeS/BPO-related matters.[134] NASSCOM acts as an "advisor, consultant and coordinating body" for the ITeS/BPO industry and liaisons between the central and state government committees and the industry.[135] NASSCOM has pioneered a range of initiatives to "build a robust Information Security environment within the ITeS BPO segments."[136]

One of the most significant efforts of NASSCOM to "establish, popularize, monitor and enforce privacy and data protection standards for the Indian ITeS-BPO industry" has been creating the Data Security Council of India ("DSCI"), a self-regulatory organization, as part of its Trusted Sourcing Initiative.[137] The DSCI focuses on providing a high standard of security and data protection, evolving and ensuring compliance with the Code of Conduct[138] and "promoting a culture of privacy and security through education and outreach."[139] It also aims at devising and enforcing ethical standards and best practices to match international standards, as well as certifying the companies that adopt the above standards and practices.[140]

NASSCOM's 4E Initiative, which aims at making India a trusted destination for Global Data Outsourcing, focuses on creating awareness, and an accountability framework through the four pillars of: "Education (and training), Engagement (with industry stakeholders), Enactment (in legislative terms) and Enforcement (through contractual and judicial compliance mechanisms)."[141]

---

134. Sylvia Carr, *India to Tighten Off-shoring Data Security*, CNET NEWS (May 9 2006, 9:57 AM), http://news.cnet.com/India-to-tighten-offshoring-data-security/2100-1011_3-6070186.html.

135. NASSCOM, *Annual Report* (2007-08), http://www.nasscom.in/upload/Annual_Report07-08.pdf.

136. NASSCOM, *Information Security Environment in India NASSOM Analysis*, (July 2006), http://www.nasscom.in/upload/5216/Indian%20Security%20Environment%202005-06%20July%2006.pdf.

137. *Data Security Council of India (DSCI): A Self Regulatory Initiative in Data Security and Privacy Protection*, NASSCOM, http://www.nasscom.in/Nasscom/templates/NormalPage.aspx?id=51973 (last updated Dec. 4, 2008).

138. *Id.* ("DSCI shall adopt the best global practices, drawing upon U.S. laws, the European Union Directive and Safe Harbor Framework, OECD guidelines, and Asia Pacific Economic Cooperation Framework in designing the Code of conduct. . .).

139. *Id.*

140. *Id.*

141. Europe India Chamber of Commerce, *Newsletter* (Nov. 2008), http://www.eicc.be/NewsLetters/NL2008/11_Nov_2008.pdf.

NASSCOM initiated the National Skills Registry ("NSR"), "a web-based system hosting a fact sheet of information about existing and prospective [employees] of the Indian IT & ITeS/BPO industry."[142] The information uploaded is comprised of personal information, academic qualifications, and work experience - the access to which is controlled by the individual. This institutionalized mechanism through which objectively verifiable data of an individual is independently checked, is a credible source of information about the IT Professionals ("ITPs") who the IT & ITeS/BPO industry and its clients employ or put on client assignments.[143] This initiative seeks to promote the BPO "industry's rightful claim for bigger share of global business on one hand and [reduce] the cost of repetitive background checks on [ITPs]."[144] NASSCOM has also initiated a "CAT exam of the BPO industry," which is a certification system for BPO employees, to "create an industry standard, which will ensure the transformation of a trainable workforce" and also "protect their employers against frauds and scams."[145]

2.2.3 *Network security*

A survey conducted shows "a paradigm shift in network security measures in the wired world from 'denial of access' to granting access to all on a 'need to know' basis."[146] The survey also showed that "importance [is] being given to access controls and stronger means of authentication" such as "dual factor authentication," "one time passwords," and "digital signatures."[147]

Encryption is another measure used to protect data from being intercepted while moving over public networks. Even though using encryption is currently relatively low, the use of encryption has increased since 2000, and "[t]he encryption technologies used in India are in line with internationally accepted levels of encrypted traffic."[148]

---

142. *Data Security Council of India (DSCI): A Self Regulatory Initiative in Data Security and Privacy Protection*, NASSCOM, http://www.nasscom.in/Nasscom/templates/NormalPage.aspx?id=51973 (last updated Dec. 4, 2008).

143. *Id.*

144. *Id.*

145. Indrajit Basu, *Indian BPO Providers Tighten Data Security*, INFIXION MEDIA (Nov. 8 2008), http://www.packagingreview.imix.co.za/node/50689.

146. Brian Pereira, *Information Security: A New Approach*, NETWORK MAGAZINE (Apr. 2003), http://www.networkmagazineindia.com/200304/cover1.shtml.

147. *Id.*

148. *Id.* Secure Sockets Layer (SSL), public key infrastructure technologies, single sign on (SSO) tools etc are some of the widely used technologies for Web-based encryption. *Id.* The use of encryption technology has been disapproved by critics. Nimmer, *supra* note 22. Some hold that it cannot be true that encryption technology can reinstate absolute personal privacy. *Id.* A technological solution to a social problem seldom works without correspond-

BPOs also ensure that a firewall exists between its Internet gateway and its local area network, thereby preventing the exposure of the corporate network to possible attacks from the Internet. Apart from these security systems, some BPOs are making use of content filtering tools, event logging and monitoring technologies, intrusion detection systems, and vulnerability assessment tools in order to protect the internal network and the data contained from external threats.

2.2.4 *Case Study: Security Measures in Wipro*

Wipro call centers utilizes physical, network, and personnel security.[149] Physical security methods include: security fencing, requirements that all visitors obtain photo-ID badges and access cards, inspection of all handbags upon entry and exit, closed circuit monitoring, and palm and retina scanners for access to highly sensitive areas.[150] Further, "employees are prohibited from carrying mobile phones or any other type of mobile storage devices, and all ports and devices that can be used to transport data outside of the center are disabled."[151] Network security measures include "implementation of the network, thorough event logging, complete set of monitoring tools, state of the art intrusion detection tools, and completely updated encryption technologies and secure connections."[152] Personnel security methods include conducting intensive background and reference checks of potential employees and requiring that employees sign confidentiality agreements.[153]

2.2.5 *International Certification Standards*

The Data Exporters require Indian BPOs to have legal understanding of and compliance with international laws and guidelines.[154] As a result, Indian BPOs are complying with a variety of international security standards, and the DPA in U.K.[155]

Data Exporters are requiring that BPOs obtain certification in accordance with international certification standards, because the IT Act of

---

ing changes in the attitudes. *Id.* What encryption can do is protect or authenticate individual messages or systems against unauthorized intrusions. *Id.*

149. Patel & Conners, *supra* note 3.

150. *Id.*

151. *Id.*

152. *Id.*

153. *Id.*

154. Ryder & Madhavan, *supra* note 64.

155. *See Security Compliance Systems*, CORAL ESECURE, http://www.coralesecure.com/security-management-compliance-systems.asp (last visited Oct. 24, 2010); *See also* Patel & Conners, *supra* note 3 ("Compliance with these laws is particularly important when with offshore work due to punitive penalties attached to non-compliance").

2000 is considered inadequate protection.[156] Compliance with these certification standards help identify, manage, and reduce the range of threats to which data is continually exposed. Once adhered to, these standards provide the Data Exporters the assurance and satisfaction of knowing that their data is protected by controls commonly used by well-managed businesses.[157]

2.3 Need for Data Protection in Indian BPOs

The outsourcing of business processes started in India with the transfer of personal data from the U.S. "without the complications that arise where cross-border transfer restrictions apply."[158] However, when the E.U. entered into the outsourcing bandwagon, the requirements regarding the protection of data became stricter, as compared to those in the U.S. The E.U. Directive, inter alia, prohibits the transfer of personal data from within the E.U. to outside the E.U., except when the certain requirements are met.[159]

The requirement of "adequate" data protection law for transferring data to a particular nation has highlighted the need for stricter data protection laws. India is considered to be a country with "inadequate" data protection laws.[160] An increased amount of outsourcing business from the E.U. "would grow drastically if India made it to the list of countries with 'adequate' data protection laws, or otherwise conformed to the requirements for lawfully hosting data from the E.U."[161] Otherwise, the Data Exporters are considering Eastern European countries, such as the Czech Republic, Russia, Romania, and Hungary, "as out-sourcing alternatives to India" because these countries may provide better data protection and better economies than in India.[162]

Most companies have their own specific standards, but there is no industry-wide framework. There needs to be a comprehensive set-up to ensure that basic measures are adhered to by all. Lack of stringent data protection laws makes the BPO scenario in India appear to be threatening to the Data Exporters abroad. "There is an urgent need to provide a protected environment for data and privacy for IT and ITeS/BPO sector

156. Birjinder Anant, Benny Kuruvilla & Meena Menon, *When the Wind Blows: An Overview of Business Process Outsourcing in India*, Focus on the Global South, India (Sept. 2005), *available at* http://focusweb.org/images/stories/pdf/bpo.pdf.

157. BS7799 and ISO 17799 Awareness: Conclusions, BS 7799, http://www.induction.to/bs7799/conclusions.htm (Mar. 18, 2009).

158. Bender, *supra* note 13.

159. *Id.*

160. European Commission, Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries (Mar. 27, 2009).

161. Bender, *supra* note 13.

162. *Id.*

in India, through the establishment of rules and standards that promote ethics, quality and best practices."[163]

With the advancements in digital and electronic technology, bringing in a fashion of use of portable devices, communication devises,[164] and other data transfer mechanisms, security of data has become the need of the hour. "[A] single instance of information security breach can tarnish the entire industry's image and the country's reputation as a safe destination for data."[165] When compared to the costs incurred in an instance of loss or misuse of data, some of which could run into millions,[166] and the loss of reputation in the market, the cost of investing in information security systems seems inconsequential.

2.3.1 *Source of Threat to Data Security*

The threat to data arises, mainly, from three sources: (1) from persons misrepresenting themselves to belong to call centers or BPOs and thereby gaining access to data stored in the database of the BPOs or even gaining access to information directly from the data subject; (2) misuse of data by the agents or employees of the BPOs who have easy access to the data in the BPOs; and (3) hacking and cyber-squatting that enables external access to the data through illegal means. In order to better address these issues, more comprehensive laws need to be in place so that there is no loss or damage to data.

2.3.2 *Case Study: Instances of Data Fraud*

Several recent cases of fraud in the Indian BPO industry have been highly publicized. For one, in early April of 2008, four employees of

163. *Data Security Council of India (DSCI): A Self Regulatory Initiative in Data Security and Privacy Protection*, NASSCOM, http://www.nasscom.in/Nasscom/templates/NormalPage.aspx?id=51973 (last updated Dec. 4, 2008) ("NASSCOM has been proactive in pushing this cause for ensuring that the Indian Information Security environment benchmarks with the best across the globe. As a part of its Trusted Sourcing initiative, NASSCOM is in the process of setting up the Data Security Council of India (DSCI) as a Self Regulatory Organization (SRO) to establish, popularize, monitor and enforce privacy and data protection standards for India's ITeS-BPO industry"). EUROPEAN COMMISSION, COMMISSION DECISIONS ON THE ADEQUACY OF THE PROTECTION OF PERSONAL DATA IN THIRD COUNTRIES (Mar. 27, 2009).

164. *See* Information Technology (Amendment) Act, 2008, No. 10, Acts of Parliament, Section 2(ha), 2009 (India) (defining "Communication device" to mean cell phones, personal digital assistants or combination of both or any other device used to communicate, send or transmit any text, video, audio or image).

165. *Data Security Council of India (DSCI): A Self Regulatory Initiative in Data Security and Privacy Protection*, NASSCOM, http://www.nasscom.in/Nasscom/templates/NormalPage.aspx?id=51973 (last updated Dec. 4, 2008).

166. *India Prepares Data Protection Laws to Aid Outsourcing*, OUT-LAW NEWS (Oct. 10, 2003), http://www.out-law.com/default.aspx?page=3970.

MphasiS used information acquired at work to steal about 450,000 U.S. dollars from the accounts of U.S.-based customers of Citibank.[167] Over the course of four months, these individuals opened several fake bank accounts and electronically transferred money.[168] They changed the account holders' e-mail addresses so that those account holders would not receive the notifications of the electronic transfers.[169] It was uncovered that these four employees worked with other perpetrators, including ex-employees of MphasiS.[170] Ultimately, sixteen people were arrested for these crimes.[171]

In another case, a sting operation by a British tabloid, *The Sun*, revealed that a BPO employee in Delhi sold a *Sun* reporter confidential information regarding the bank accounts, credit card details, and personal data of 1,000 British customers for over 4,000 U.S. dollars.[172] In another sting operation in August 2005, by Australian Broadcasting Corporation, it was reported that the employees of a BPO in Gurgaon sold the personal information of over 1,000 Australians at ten dollars per person.[173]

3. APPROACH TOWARDS BETTER PROTECTION OF DATA

3.1 Suggestions for Data Protection in BPOs in India

> The goal of a data protection program must be:
> to avoid costly law suits and embarrassment in public relations incidents that may result from revealing information that is protected by law, that management has determined could be detrimental to the enterprise if known by the competitors of the public or that customers [and employees] feel should be kept private.[174]

As recognized by NASSCOM, "successful security solutions require a convergence of the three components, viz. people, technology, and processes."[175] An attempt has been made to propose solutions for better data protection, under each of these three components.

---

167. *Indian BPO Providers Tighten Data Security*, Offshoring Times, http://www.offshoringtimes.com/Pages/2005/Content233.html (last visited Oct. 24, 2010).

168. *Id.*

169. *Id.*

170. *Id.*

171. *Id.*

172. Oliver Harvey, *Your Life for Sale*, The Sun (June 23, 2005), *available at* http://www.thesun.co.uk/sol/homepage/news/article108989.ece.

173. *INDIA: BPO's Do it Again, Aussie Data on Sale*, Times of India (Aug. 16, 2005), *available at* http://www.asiamedia.ucla.edu/article.asp?parentid=28294.

174. Michael Erbschloe & John Vacca, Net Privacy xvii (2001).

175. *Data Security Council of India (DSCI): A Self Regulatory Initiative in Data Security and Privacy Protection*, NASSCOM, http://www.nasscom.in/Nasscom/templates/NormalPage.aspx?id=51973 (last updated Dec. 4, 2008).

3.1.1 *People-related Security Measures*

Employees are the most integral parts of a BPO. While their presence can make a BPO flourish, at the same time they may be potential threats to the BPO, thereby calling for stringent security measure provisions. Although it is important to achieve high security standards, these security measures must be conducted without causing inconvenience to and harassment of employees.

Interplay between employment and data protection policies can be regulated in several aspects. When a BPO seeks to recruit a person as an employee, whether temporary or permanent, the credentials of the prospective employee must be thoroughly checked. BPOs must take the employee screening seriously. The Human Resource department plays an important role in conducting a background check of the current and potential employees. At the time of recruitment, the employee must be required to give details regarding criminal records and medical history. All details about the prospective, current and former employees must be recorded and retained. These details may include the name, contact details, family background, responsibilities held/to be held, reasons for termination of employment, past job experiences and reference details, to name a few. Policies regarding management and disclosure of employment data to external parties, such as the following, must be in place:

Data matching. A system,[176] whereby, any impeaching information that is found against a person/employee may be fed into a common server and accessible by all employers and recruiters, would reduce the time and costs spent in conducting background checks.[177]

Training. The most important requirement for vigilance on data is that the employees must be trained and educated about their obligations and the rules and penalties in case of non-compliance. Seminars, presentations, workshops, and recovery drills may be held from time to time, not only for the employees but also for the employers.

Safety of employees. Protection of data starts with the safety of the persons handling the data. There have been many instances where the safety of a company employee has been threatened because that person holds an influential post and has access to the records and information

176. "Data matching" is the system of cross-reference of information from diverse sources. This system has been met with polarized reactions, where on one hand it is considered to be a cost-effective method of locating resources and enforcing regulation, but on the other hand, it is considered to be intrusive. Kenneth J. Langan, *Computer Matching Programs: A Threat to Privacy?*, 15 COLUM. J L. & SOC. PROBS. 143 (1979). This system is mainly followed in the federal agencies in the US. A similar strategy may be adopted in the context of Indian BPOs.

177. An initiative has been taken by NASSCOM in this regard, as discussed *supra*.

of the company.[178] There is a need to protect the employees of these companies/BPOs who hold higher posts and have greater responsibility within the company, so as to reduce their exposure to external threats.

Staff monitoring. In order to maintain and monitor internal activities, the BPOs must install CCTVs and employee monitoring policies. The use of line managers, private detectives, etc., must be encouraged for risk management and monitoring staff activities and communications.

Employee retention measures. The phenomenon of attrition,[179] faced by BPOs, weakens the relationship between the employer and the employee. This could lead to deflated loyalty towards the company, thereby increasing instances and grounds for infidelity by the employees. Therefore, taking measures to lower attrition rates will help build employee confidence and loyalty towards the BPO and the employers.

3.1.2 *Technology-related Security Measures*

Security, in a technical form, should be given more importance than control over behavioral tendencies and disaster management. Data protection must be reached through, what may be called, device management measures. According to one study,[180] "most proactive companies now encrypt all portable data. . .while leaving all in-house data intact."[181] However, loss or damage to in-house data may be as harmful as loss or damage to outsourced data and they should not be excluded from protection. Moreover, data security products must be made easily available at affordable prices, so that even small enterprises may have the benefit of data security. Below are a few examples:

Data "redaction." Another solution is data "redaction," where only part of the data field, i.e., the credit card number, date of birth, telephone number etc, is displayed on agents' or employees' screens. The data subject must be given control over the data by way of data key or

178. *BPOs Told to Adopt Best Security Norms for Safety of Employees*, FIN. EXPRESS (Dec. 12, 2005), http://www.financialexpress.com/news/bpos-told-to-adopt-best-security-norms-for-safety-of-employees/154987/.

179. *See* Sanjeev Sharma, *High Attrition Rate: A Big Challenge*, BPO INDIA, http://www.bpoindia.org/research/attrition-rate-big-challenge.shtml (last visited Oct. 24, 2010) (defining attrition as "[a] reduction in the number of employees through retirement, resignation or death"). The average attrition rate in the BPO industry in India is approximately thirty to thirty-five percent. *Id. See also Human Resources Issues in BPO*, BPOWATCH INDIA, http://www.bpowatchindia.com/HR_outsourcing.html (last visited Oct. 24, 2010) ("Repetitive low-end jobs, physical and psychological problems and inadequate growth opportunities are the major reasons cited for the high attrition rate. This disadvantage has increased the operating costs of BPO entities and is considered to be a threat to the growing industry").

180. Allan Holmes, *Your Guide to Good Enough Compliance*, CIO MAG. (Apr. 6, 2007), *available at* http://www.cio.com/article/102751/Your_Guide_To_Good_Enough_Compliance.

181. Patel & Conners, *supra* note 3.

password. The complete details are made accessible to the agent or employee only on seeking permission from the data subject and only when the data subject himself discloses the necessary information on accessing the data on using the password. This way the data is completely under the control of the data subject.

Back-up storage sites. Infosys, a leading BPO in India, maintains back-up storage sites outside of India.[182] As a precaution, client data is transferred at regular intervals to these "offshore" facilities so as to provide exclusive backup facility for each of its clients.[183] This innovation should be given serious consideration by other Indian BPOs. This way, the data will receive protection against loss due to network or security breakdown.

E-waste and paper disposal. There is a threat of dissemination of data through e-waste and paper. Proper disposal of e-waste is most important. An ink and paper-free work place, accessibility of paper disposal and shredding equipment and controlled printing are suggested.

3.1.3 *Processes-related Security Measures*

In order to ensure adequate protection of data, it is not only important to implement the three above-mentioned measures but also to identify the means by which they may be achieved. Processes-related security measures may be designed to ensure the proper working of the components for efficient data protection, and may be further divided into industrial code of conduct and statutory measures.

3.1.3.1 *Industrial Code of Conduct*

A policy for the protection of data in the BPO must be consistent with (a) the business operations and legal compliance requirements, (b) management goals and the culture of the company, and (c) the company's technology infrastructure.[184] Keeping these in mind, the BPOs can develop a scheme for data protection by identifying and addressing issues concerning how the company will perform the following tasks:

regulate privacy matters, including accountability and ownership issues;

determine its requirements, including its contractual, regulatory and policy requirements;

handle its data, including acquisition, use, storage, sharing and distribution, management, retention and destruction of the data;

---

182. *Id.*

183. Jaikumar Vijayan, *Security Expectations, Response Rise in India*, COMPUTERWORLD (Aug. 20 2004), http://www.computerworld.com/s/article/95533/Security_Expectations_Response_Rise_in_India.

184. JODY R. WESTBY, INTERNATIONAL GUIDE TO PRIVACY (2005).

> adopt an appropriate taxonomy for the company, including defining personal and sensitive information, secondary usage and access in the context of the BPO's operations;
>
> develop appropriate policies and procedures that align with the BPO's culture, people, processes and technology;
>
> implement its policies and procedures, including training, standards guidelines and audits;
>
> monitor, evaluate and adapt the policy based on changes in the brand, culture, technology and information systems, contractual and regulatory requirements; and
>
> cope with disaster management and recovery procedures.[185]

A thorough step-by-step approach will enable a BPO to fabricate a scheme of data protection policy, which can help lure the Data Exporters to India.

Asset and risk identification. First, the data, which is to be protected, must be identified and categorized on the basis of degree of protection needed. The BPO must also identify various risks involved, including "technology risks" and "people risks." It is important to maintain transparency about the security measures in a BPO in order to market itself as more attractive to foreign clients.[186]

Internal data management system. "Employing certified security professionals to safeguard the data would prevent possible breaches of security."[187] Furthermore, the BPO must have an internal management team that communicates and coordinates across the company. The responsibilities of each member of the team must be clearly determined along with specifications as to timelines, reviews, and reports. This team must play an integral role in ensuring execution of and compliance with the BPO's data protection and security policy.

Contractual Measures. The contractual measures to be taken must be addressed at two levels. First, contracts between the Data Exporter and the Indian BPO need to be safeguarded. Second, the contracts between the Indian BPO and its employees need to be addressed so as to bind the employees to maintain confidentiality and uphold the employers' obligations towards the Data Exporter and the data subjects, with sanctions in the event of a breach.

The analysis of the possibilities of harnessing the phenomenon of the international transfer of personal data by contractual clauses in the context of contract law has unraveled a number of weaknesses within the system. In order to ensure a concrete framework in relation to trans-

185. *Id.*
186. Patel & Conners, *supra* note 3.
187. *Id.*

border transfer of data, a uniform, systematic and comprehensive law on contractual clauses in this regard needs to be developed. Addressing the shortcoming regarding the dispute resolution clause, the contract entered into between the BPO and the Data Exporter must include a provision that any third party would also be bound by the same dispute resolution clause stated in the contract.

In the case of loss or damage to the data subject, the data subject must have the right to hold each of the parties to the contract "jointly and severally" liable for the loss or damage caused. For the loss or damage caused by one of the parties, the other will be liable for making reparation where the one causing the loss or damage, fails to do so. The rules governing liability are not identical in every country. Some countries may not grant damages for non-pecuniary damage and sometimes it might be difficult to obtain such damages under contract law. Provisions of regulations governing outsourcing contracts regarding personal data will give rise to a specific action for non-pecuniary damage in case of breach thereof.

Outsourcing contracts include references to third parties or the data subjects and the obligations of the data importer towards the third party or the data subject. However, the data subject cannot be in control of his data and cannot realize his rights until he is completely aware of his rights under the outsourcing contract. Hence, it is important that the data subjects are notified of the fact that they are covered by the outsourcing contract, so that they may exercise a right to opt-out of the arrangement. Sub-contracting by the BPO needs to be addressed in an outsourcing contract between the Indian BPO and the Data Exporter and such sub-contracting is to be in accordance with the data subject's rights and the outsourcing contract.

Assessment of the performance. There must be frequent measurements of the performance, similar to daily performance and operation of the company, through sophisticated status tracker, self-assessment tools, and customer feedback systems. Only when the performance of the company is assessed, can measures for its improvement be taken. Furthermore, there must be periodic assessment of the performance and effect of security measures internally in the BPO.

Intellectual property due diligence. Data Exporters often use due diligence inquiry on the BPO proposed to handle its data. A system of domestic intellectual property due diligence inquiry must be introduced in India that would satisfy two purposes. First, it would help the BPO assess its security standard and consequently strive to achieve better standards. Second, and most importantly, it will project the company profile and the market atmosphere that the Data Exporter expects.

3.1.3.2 *Statutory Measures*

Regulatory requirements. India may adopt a co-regulatory model,[188] similar to those of both the U.S. and the U.K. However, there must also be sector specific rules. This dual safeguard will place higher standards of protection of data transfer.

Sui generis protection of data. In order to have continued trade with the E.U., it is important that there is adequate legislation in India, which incorporates the eight basic principles that are the essence of the E.U. model. The legislation must provide a minimum standard of protection of data and must establish the basic requirements for compliance with international standards. In order to achieve this, the legislation must address all the terms and concepts relevant in the Indian context, including those of personal and sensitive data, data collector, and rights, duties, and liabilities of the concerned parties.

Specially trained judges. In the field of data protection, there should be a selection of judicial officers specifically trained to deal with intellectual property violations. The Cyber Appellate Tribunal, presently constituted under the IT Act of 2000 is composed of only one person who acts as the Presiding Officer of the Tribunal.[189] There must be a provision for engaging an advisor or an independent consultant to adjudicate certain matters before the Tribunal.

Shift from ADR to ODR. The most basic and well advocated[190] solution to enforcement and resolution of the issues is addressing the current court's burden, delay, and costs, and ensuring prompt conclusion of cases with deterrent penalties and compensatory damages. However, this is easier said than done. Steps must be taken to set up an efficient system of Online Dispute Resolution ("ODR"). This would improve access and help trans-border settlement of disputes. A hierarchy of ODR mechanism must be set up on the basis of amount of damages or compensation claimed and/or type of security breach. There must be rules and laws in place with regard to examination of evidence through the electronic medium. Only where the adjudicatory authority feels it absolutely necessary, in the interest of justice, should it recommend the dispute to arbitration or litigation.

International cyber infringement courts. Specialized international cyber infringement courts could be established, with jurisdiction

188. Ryan Moshell, *And Then There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection*, 37.2 TEX. TECH L. REV. 357 (2004).

189. Information Technology Act, No. 21 of 2000, INDIA CODE, Section 49.

190. Hiram E. Chodosh, Stephen A. Mayo, A.M. Ahmadi & Abhishek M. Singhvi, *Indian Civil Justice System Reform: Limitation and Preservation of the Adversarial Process*, 30 N.Y.U. J. INT'L L. & POL. 1 (1998).

over all violations related to intellectual property across the globe.[191]

Data policing. There must be a national set-up for implementation and enforcement of the data protection provisions, examination of crimes related to data, and training in electronic data piracy and enforcement.[192]

Cyber Security Policy. A strong Cyber Security Policy is desirable in India at the wake of the technology revolution by way of the acceptance and adoption of Information and Communication Technology and its benefits. An ideal Cyber Security Policy "presupposes the existence of a sound and secure e-governance" and "the adoption and use of security measures, more particularly, [training] the judiciary and law enforcement manpower with the knowledge and use of Cyber Forensics and Digital Evidencing."[193]

Law regarding surveillance. Growing awareness for data protection and development of technological systems has led several countries to find it "necessary to draft specific legislative provisions on data protection in the field of video surveillance."[194] However, it is a pertinent caution to avoid either overlapping and rigidity of laws or excessive generality in the legal framework. India must evaluate and prioritize the effects resulting from the widespread use of surveillance with regards to citizens' freedom of movement and behavior.

---

191. *See* Bali, *supra* note 54, at 41, fn 113. ("Given the cross border nature of breaches, and the ever increasing global interactions pertaining to intellectual property (including data privacy), these international tribunals may be an appropriate and effective solution in the future. . .This model may be drawn from the Council of Europe's Convention on Cybercrime. . .[which] requires parties to have the ability to investigate computer-related crime effectively and to obtain electronic evidence in all types of criminal investigations and proceedings. By providing for broad international cooperation in the form of extradition and mutual legal assistance, the Cybercrime Convention is intended to remove or minimize legal obstacles to inter-national cooperation that delay or endanger a State's investigations and prosecutions of computer-related crime" (citations omitted)).

192. Advancement has been made in this regard by establishment of cyber crime police stations in the cities of Mumbai, Bangalore and Hyderabad. *See* Mateen Hafeez, *City to Get First Cyber Crime Police Station*, TIMES OF INDIA (Apr. 4, 2009), http://timesofindia.indiatimes.com/Mumbai/City-to-get-first-cyber-crime-police-station/articleshow/4360070.cms.

193. Praveen Dalal, *Cybersecurity in India: An Ignored World*, COMPUTER CRIME RESEARCH CENTER (Feb. 7, 2007), http://www.crime-research.org/articles/Cybersecurity-India-Ignored-World/.

194. Giovanni Buttarelli, *Protection of personal data with regard to surveillance and Guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance*, COUNCIL OF EUROPE (2000), *available at* http://www.coe.int/. . .%20experts/1Report_Buttarelli_2000.pdf. ("Based on the technical development of these systems, it has progressively become possible to transmit images to a 'control centre' from terminals connected either via cable, optic fibers or digital network; to record images other than via CCTV (closed circuit television); to obtain images with higher resolution and reproduce them in color; to associate images and sound; to expand the visual field up to a 360 degree vision; . . .to use zooming functions. . .").

CONCLUSION

Data Protection: An Optimistic Approach

On a critical examination of the Indian BPOs' data protection, one may question whether the protection offered is really insufficient and "inadequate." According to NASSCOM, the current environment suggests that most Indian BPOs have made positive changes.[195] All member companies are compliant with international certification standards, IT Act of 2000, Copyright Act, Contract Act of 1957 and IPC, and provide adequate protection for data security. The concerned BPOs are even adhering to the HIPAA, GLBA, and Data Protection Act of 1998 at the request of their respective clients.[196]

The absence of a single consolidated law on data protection has bred a misconception that India lacks sufficient data protection provisions. An unbiased examination of the data protection provisions in India, including the various self-regulatory practices and initiatives, tilts the balance towards adequacy of protection. The IT Act of 2000 does address the major issues that a new law on data protection is expected to do. For example, the IT Act of 2000 recognizes both civil and criminal penalties for "any attack on data" and also provides for the "technical facilitation of data protection" and processes for addressing grievances.[197]

There are ongoing efforts to keep the Indian BPO industry on par with international expectations. NASSCOM is the major body that is lobbying on behalf of the Indian BPO industry.[198] There are also special groups like Special Interest Group for IT Enabled Services, the Confederation of Indian Industry, and the Federation of Indian Chambers of Commerce and Industry. The Associated Chambers of Commerce and Industry of India ("ASSOCHAM") also has an initiative to specifically promote the BPO industry. The ASSOCHAM has "formed a BPO Steering Committee with representation of industry chieftains, analysts and experts in this field," and "also proposes to form a one-stop information help-desk for all Indian and international companies seeking to know

195. NASSCOM, *Annual Report* (2007-08), http://www.nasscom.in/upload/Annual_Report07-08.pdf.

196. A study by *Price Waterhouse Cooper* and *CIO magazine* found that despite the perceived lag in data protection protocols, Indian BPOs are finding ways to improve their security measures. Confederation of Indian Industry (CII) & PricewaterhouseCoopers, Information Security Survey (2002-2003). These companies are outspending their counterparts in other nations by almost thirty percent on data security. *Id.*

197. *India Has a Robust Data Protection Law*, Naavi (June 25, 2005), http://www.naavi.org/cl_editorial_05/edit_june_24_05_01.htm.

198. NASSCOM has over 1200 member companies, which accounts for over ninety-five percent of software industry revenues in India. *About NASSCOM*, NASSCOM, http://www.nasscom.in/nasscom/templates/normalpage.aspx?id=5365 (last visited Mar. 16, 2009).

more about the [Indian BPO] industry."[199]

The concerted efforts of India have not gone unnoticed. Despite the perceived lag in protection of data and stray cases of data fraud, India is home to some of the biggest software and hardware production enterprises. While there is room for growth and improvement, the competition is increasing because many countries have created thriving business environments. Hence, resolute efforts are required to address the current challenges, to ensure that India realizes its potential and maintains its leadership position through cost-effective and faultless compliance processes.

199. ASSOCHAM, http://www.assocham.org/bpo/ (last visited Oct. 24, 2010).