HOW PROTECTED IS ELECTRONICALLY TRANSFERRED DATA FROM BUSINESS PROCESS OUTSOURCING (BPO) UNITS – THE INDIAN SCENARIO

R.Raman
Assistant Professor-Kohinoor Business School, Khandala , Affiliate Professor - Sprott School of Business, Carleton University- Ottawa, Canada
&
Parag Waknis
Research Scholar, University of Connecticut- Connecticut, United States of America

ISSN – 14
Year December 2007 Volume 1, Issue 4/4

Abstract: *India is one of the most preferred destinations for outsourcing[1]. The main reason for this is abundant availability of labour at a very low cost[2]. As the companies around the globe are looking at India as the destination for outsourcing, the issue of information piracy and data security in India has come become a vital issue.*

The United Kingdom's Labor party Members of European Parliament affiliated with the Amicus trade union in the United Kingdom announced that they would ask the European Union's executive branch, the European Commission, to protect ***British consumers whose personal data is being transferred to India, warning that offshore outsourcing is "an accident waiting to happen."*** *[3] Against this background* ***this paper tries to find, if with the current statutory measures, policies and cyber laws that exist in India, can India provide adequate protection for electronically transferred data for the outsourced projects and explores the possible changes that can be made to improve upon the same.***

Keywords*: BPO, Outsourcing, Information Piracy, Data Security, Statutory Measures, IT ACT 2000.*

---

1 www.Nasscom.org

2 Rajas Kelkar(2002), "India, Ireland Turn Outsourcing Hubs" The Economic Times,20th December 2002, p1.

3 John Ribeiro(2004), "*Indian Law May Satisfy EU Data Protection Concerns"*, COMPUTERWORLD, 21st April, 2004,

Methodology of the study

This research paper is based on the secondary data available from Department of Information Technology, Ministry of Communications & Information Technology, and Government of India websites. Also the data available from different sections of Indian Penal code, data from The World Trade Organization (WTO) Agreements on Trade-Related Aspects of Intellectual Property Rights (TRIPs), Policy Statements on Intellectual Property Rights in India and other literature available online by different authors who have carried out research on the data security issues have been used. Also views from CEOs' of different outsourcing companies have also been taken into consideration to get understand the problem from the real time business perspective.

Introduction – Why Is Protection for Electronically Transferred Data Important?

Caselet [4]

The Indian offshore outsourcing industry was rocked by the revelation that call centre workers in Pune were arrested for allegedly looting $350,000 from the accounts of Citibank's US customers. The three staff members were the former employees at Indian business process outsourcing (BPO) firm Mphasis, which runs call centre services for Citibank's US customers in Bangalore and Pune.

The former Mphasis staff used their positions dealing with Citibank's customers to trick four of them into giving out the PIN numbers to their accounts, allowing the staff to transfer funds into the bank accounts of other their gang members. The fraud was only discovered when the customers noticed the money missing from their accounts and Citibank subsequently traced it back to the Mphasis operations in Pune. Mphasis said it "regretted" the incident, but maintained that its security procedures are adequate.

This case-let which explains why protection for electronically transferred data is important. The center in Pune was BS 7799 and CMM Level 5 certified (Quality Certifications), but still, the breach occurred. This case-let also emphasizes that security complacency is not for sure given, just by list of certifications or process changes that companies roll out. Also this case-let reveals that there is definite need for security and integrity for the electronically transferred data, also a proper legal framework is a must for achieving the same. ***Hence statutory measures*** for BPO operation in India is ***becoming increasingly important*** and ***a cause of great concern*** to investors, corporations, the legislature and the public in other nations

Data Protection Laws in India

The reality is that India does not currently have any specific data protection law. Data protection and privacy are given scattered and rather sparse coverage by existing laws. The existing data protection laws, in India, are scattered in laws pertaining to information technology, intellectual property, crimes, and contractual relations. Under increasing pressure from BPO operations and call centers in India that handle large volumes of data from the US and Europe, the government of Indian is contemplating a comprehensive law for protecting data that are sent over the network of networks.

Despite the criticality of the matter and demands from internal and external fronts, India has delayed enactment of

---

4 http://www.silicon.com/research/specialreports/offshoring/0,3800003026,39129426,00.htm

legislation for several years.[5] The form of the legislation there has been a debate and discussion over the protection for cross-border data processed in India. At this point, it appears likely that India's Information Technology Act of 2000 ("IT Act of 2000") will be amended to incorporate laws that provide comprehensive protection to data[6].The current laws in India are the only protection offered for data privacy violations. It is observed that unlike the Directive which imposes liability on each participant within the chain of command of the data who failed to protect the sanctity of the data, India's existing laws only prosecute those individuals who directly violate laws related to computer systems or copyright. Entities are exempt for breaches of data privacy unless such a violation was made knowingly. Unlike the Directive which protects data breaches by limiting its collection and use, the Indian laws do not specify conditions under which data can be collected and used. Where liability may be found by stretching the existing laws to cover breaches of data privacy, penalties afforded to victims are inadequate in the existing Indian laws.

Are there any Deficiencies in the Indian Data protection laws – Under the Transnational context?

To understand if there are any deficiencies in the Data protection laws under the transnational context the **IT Act 2000** has been taken as a case and analyzed.

The IT Act of 2000, Section 43(b) affords cursory safeguards against breaches in data protection[7].The scope of Section 43 (b) is limited to the unauthorized downloading, copying or extraction of data from a computer system, essentially unauthorized access and theft of data from computer systems. Section 43(b) is limited in scope, and fails to meet the breadth and depth of protection that the EU Directive mandates. The law creates personal liability for illegal or unauthorized acts, while making little effort to ensure that internet service providers or network service providers, as well as entities handling data, be responsible for its safe distribution or processing. Furthermore, the liability of entities is diluted in Section 79 of the act, which inserts "knowledge" and "best efforts" qualifiers prior to assessing penalties.[8]

A network service provider or intermediary is not liable for the breach of any third party 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 or contravention[9]. Similarly, while Section 85 of the Act does invoke entity liability, such liability is limited to the specified illegal acts under the IT Act of 2000 which does not offer broad

[5] An amendment to the IT Act of 2000, offering enhanced protection to data, was close to enactment in 2004, after 7 years in the making; unfortunately this proposed amendment was shelved due to a change of India's Central government. Andy McCue, *Offshore Data Protection Law Flounders*, SILICON.COM, *available at* http://www.silicon.com/research/specialreports/offshoring/0,3800003026,39130054,00.htm.

[6] THE IT ACT, 2000, Order under Ministry of Law, Justice and Company Affairs (Legislative Department), June 9, 2000. The IT Act of 2000 covers cyber and related information technology laws in India. It deals essentially with authentication of electronic records and electronic signatures, lacking specific provisions relating to privacy of data, data interception and computer forgery. Report of the Expert Committee, Proposed Amendments to Information Technology Act 2000, Department of Information Technology, Ministry of Communications & Information Technology, Government of India, August 2005, available at http://www.mit.gov.in/itact2000/Summary-final.doc. Also, Sufia Tippu, Indian IT Act to be Amended to Net Cyber Criminals, IT WIRE, July 13, 2006, available at http://www.itwire.com.au/content/view/4957/945/ .

[7] IT Act of 2000, *supra* note 54, at Ch. IX Section 43(b).

[8] IT Act of 2000, *supra* note 54, at Ch. XII Section 79.

[9] IT Act of 2000, supra note 56, at Ch. XII Section 79.

protection of data[10].Section 85 does extend liability to key employees (managers, directors, officers etc) of the company for intentional or negligent acts that result in a breach of the specific violations under the IT Act of 2000[11].

With regard to damages available in the event of a breach of data privacy, Section 43(b) is deficient in that the maximum penalty for this breach is monetary compensation in the paltry amount of approximately two hundred and twenty thousand dollars ($220,000) [12]

The maximum monetary damages available for a breach that can potentially be several times more, is clearly inadequate in a transnational context. The law makes no differentiation based on the intentionality of the unauthorized breach, and no criminal penalties are associated with a breach of Section 43(b). The more limited crimes of computer hacking and tampering are considered criminal offenses under the IT Act of 2000: Section 65 offers protection against intentional or knowing destruction, alteration, or concealment of computer source code with. Section 66, while offering no clear language which protects personal data, offers limited protection when personal data is destroyed, deleted or altered. Both Sections 65 and 66 are punishable with criminal penalties including jail time of up to 3 years or a monetary penalty of up to $440,000.[13]

In addition to Sections 65 and 66, although Chapter XI of the IT Act of 2000 specifies criminal penalties for a laundry list of illegal acts, no such recourse is available for the broad realm of breaches of personal data security. In addition to the protections discussed above, Section 72 of the IT Act of 2000 offers some protection for breaches of confidentiality and privacy.Non-consensual disclosure of confidential information is punishable by imprisonment for up to 2 years, or a maximum fine of approximately $220,000 [14].In contrast to the IT Act of 2000, the European Union (EU) Directive envisions much broader violations associated with breach of data security than does the limited sphere of the IT Act 2000. EU Directive provides for protections in the entire chain of control of data, and creates systems of security and associated penalties within the various stages of data processing[15]

For instance, the Directive prescribes limits to the collection of personal data, requiring that a purpose for the data collection be articulated. The 1980 Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data promulgated by the Organization for Economic Cooperation and Development (OECD) are also instructive, demonstrating that a large void exists in India's IT Act of 2000. A reformation of the IT Act of 2000 should encompass the principles contained in the Directive, and the parallel OECD principles related to limitation of data collection, data quality, specified purpose, use limitation, security safeguards, individual participation and accountability[16]. For instance, the Directive prescribes limits to the collection of personal data, requiring that a purpose for the data collection be articulated [16]. The Directive also requires that data must be obtained by lawful and fair means and, where appropriate, with the knowledge or

[10] IT Act of 2000 Ch. XIII Section 85. Section 85 (1)

[11] IT Act of 2000 Ch. XIII Section 85 (2). Section 85 (2)

[12] IT ACT 2000 Section 43(b), 43(h).

[13] IT ACT 2000 Sections 65, 66.

[14] IT ACT 2000 Ch. XI, Section 72,

[15] EU ACT Notes 20

consent of the data subject; personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date[16].

Further, in matters of trans-national data protection the IT Act of 2000 is deficient in that jurisdiction for cases arising out of violations lies in India. A special tribunal is established by the Central Government, and all matters arising out of the IT Act of 2000 are within the jurisdiction of this Cyber Appellate Tribunal[17]. While the IT Act of 2000 is diligent in establishing a tribunal headed by a qualified judicial officer, the difficulty in accessibility to this tribunal is stark in a trans-national setting. Injured parties who are non-residents of India would have to adjudicate disputes in a foreign jurisdiction, incurring the related expense ad inconvenience thereof. The limited parties, from whom recourse can be sought, limited circumstances under which remedy may be established, and the limited nature of the damages is even more when the avenues for recourse and compensatory sums are viewed from a perspective of third party nationals.

Provisions for Data Protection in the Indian criminal laws

The provisions in the Indian criminal laws and intellectual property laws doe data protection also afford limited protection for personal data. They have provisions contain many gaps making the overall existing data protection scheme in India inadequate. The Indian criminal laws do not specifically address breaches of data privacy. Under the existing Indian Penal Code, liability for such breaches must be inferred from tangentially related crimes.

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[18]. Movable property has been defined as property, which is not attached to anything, and not land: although no jurisprudence has developed on this interpretation, arguably, movable property encompasses computer-relayed data and intellectual property [19].

In addition, Indian Penal Code Section 405 provides criminal penalties for criminal breach of trust. Section 405 provides that "[w]hoever, being in any manner entrusted with property, or with any dominion over property, dishonestly misappropriates or converts to his own use that property, or dishonestly uses or disposes of that property in violation of any direction of law prescribing the mode in which such trust is to be discharged, or of any legal contract, express or implied, which he has made touching the discharge of such trust, or willfully suffers any other person so to do, commits "criminal breach of trust"." Liability under Section 405 extends to employees and agents of the violator, and the crime is punishable by imprisonment and/or fine[20]. Section 424 of the Indian Penal Code provides criminal liability for dishonest or fraudulent concealment or removal of property. Accomplice liability is also envisioned, with jail and fines imposed on the first party or accomplice[21].

---

16 http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

17 IT Act of 2000, *supra* note 54, at Ch. IX, Section 46, 47, and Chapter X, Sections 48

18 INDIA PEN. CODE Section 403.

19 INDIA PEN. CODE Section 22, 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."

20 INDIA PEN. CODE Section 405

Sections 420 of the Indian Penal Code may also offer some protection for failure to adequately protect data. Section 420 pertains to dishonest delivery of property to a third person[22]. All this indicate that the adequacy of the remedies under India's criminal laws in a trans-national context remains questionable.

Provisions in Intellectual Property laws for Data Protection

Computer software (including computer programs, databases, computer files, preparatory design material and associated printed documentation, such as users' manuals) have copyright protection under Indian laws. Computer programs per se are not patentable, being patentable only in combination with hardware[23]. Thus in India, by past practice and under current laws, copyright is the preferred mode of protect for computer software.

A 1994 amendment of the Copyright Act of 1957 brought sectors such as satellite broadcasting, computer software and digital technology under Indian copyright protection. Protection of intellectual property rights in India was considerably strengthened in 1999. In addition to major legislation pertaining to patent and trademark laws, the Indian Copyright Act of 1957 was amended to make it fully compatible with the provisions of the TRIPS Agreement[24]. Known as the Copyright (Amendment) Act, 1999 ("Indian Copyright Act"), this Act came into force on January 15, 2000.

The Indian Copyright Act prescribes mandatory punishment for piracy of copyrighted matter commensurate with the gravity of the offense. Section 63B of the Indian Copyright Act provides that any person who knowingly makes use on a computer of an infringing copy of computer program shall be punishable for a minimum period of six months and a maximum of three years in prison[25].

Fines in the minimum amount of approximately $1250, up to a maximum of approximately $5,000 may be levied for copyright infringement of computer software. An enhanced penalty is available for second or subsequent convictions-imprisonment for a minimum term of one year, with a maximum of three years, and fines between $2,500 and $5,000[26]. As with penalties under the IT Act of 2000, these penalties are inadequate in a transnational context.

Conclusion and Recommendations

Considering the above analysis and facts it is clear that there are serious issues that have to be addresses or protecting Electronically Transferred Data from Business Process Outscoring (BPO) units in India. There must be strategic change in the manner in which issues related to cyber crime and protecting Electronically Transferred are handled.

The amendments in IT Act has to be made and all crime related to cyber space must be considered and treated at par

---

[21] INDIA PEN. CODE Section 424

[22] INDIA PEN. CODE Section 420

[23] India Patent Act 2005 (http://www.managingip.com/?Page=17&ISS=17631&SID=524402)

[24] http://www.wto.org/english/tratop_e/trips_e/t_agm0_e.htm

[25] India Copyright Act, 1957, Chapter XIII, Section 63A, 63B.

[26] http://www.indianembassy.org/policy/ipr/ipr_2000.htm

with criminal and sexual crimes. The severity of punishment of punishment can to some extent prevent cyber crimes to happen. The next best way to deal with the current situation is to ***create cyber court, similar to the consumer courts*** that have been created to protect the rights of consumer. The creation of cyber courts can enable speedy punishment possible.

Also **establishment of a national centralized enforcement body** dedicated to, and trained in electronic data piracy and enforcement can do lot good in the transnational context. Apart from this the local police enforcement units which must be specifically trained and maintained to recognize instances of and enforce actions against data piracy crimes, which can be a solution at the grass root level.