Securing sensitive personal information: Biggest Predicament for IT Industry

Introduction

India is increasingly being regarded as the focal point of global IT outsourcing. The Indian IT and ITeS sector showcased a phenomenal growth during the past years despite the recent economic slump and is still considered as the most preferred outsourcing destination.[1] Despite this growth, the principal concern for the IT industry is the lack of a privacy and data protection regulation in India to preserve sensitive data. While electronic records of information provide a convenience and simplicity of procedure, yet there is the added risk of misuse of the information by unscrupulous persons or organizations. Given the quantity of processed data that is increasingly incessantly, there is a greater potential increase in the degree of risk that a misuse could pose for data and privacy.

In light of the above, this newsletter proffers to explore the existing data security and privacy protection laws and regulations in India and assess if they are sufficient for meeting the needs of the fast growing IT industry. It shall identify the impediments to the establishment of an efficient data protection regime, and also attempt to bring it par with the international data protection standards.

1.0 The Existing Regulatory Regime

Indian data protection regime operates under umbrella legislations rather than a specific coherent legislation dealing with the issue of data protection and privacy. However, one could claim that other statutes provide some safeguards to the lack of explicit legislation. These statutes must be examined even if they cannot provide adequate protection on their own accord. For financial institutions, the Public Financial Institutions Act mandates the obligation of a public financial institution for fidelity and secrecy. The Credit Information Companies (Regulations) Act puts obligation on companies regarding accuracy and security of credit information. The Consumer Protection Act provides that disclosing confidential data and not performing contractual obligation amounts to deficiency of service.[2] The Indian Telegraph Act regulates telegraphs for the transmissions of information and signals wherein the government has the exclusive power to intercept messages. However, these regulations are sector centric and do not guarantee protection to the IT industry. This also leads to multiplicity of judicial opinions, inconsistencies in business practices and uncertainty of remedies available in case of data breaches.

In practice, the Indian companies acting as the "data importers" also enter into contracts with "data exporters" to adhere to an internal mechanism of high standard of data

[1]See http://planningcommission.nic.in_ch8.pdf and http://economictimes.indiatimes.com/tech/ites/india-still-worlds-no-1-destination-for-offshore-outsourcing/articleshow/7138729.cms - visited on December 23, 2010.
[2] Smt Ramala Roy vs. Rabindra Nath Sen, 1994 (I) CPR 66.

protection and safeguard client's information. Even employees are contractually bound to protect the confidential information. Under Indian contract law, these contractual obligations dealing with data protection may be enforced. Further preventive remedies like a suit for injunction- both temporary and perpetual, are available under the Specific Relief Act to avert breach of obligations. In addition, tort law provides remedies in the form of criminal breach of trust, on the premise that confidential information is provided to an individual in trust. Under common law, a civil action can also be brought for securing damages due to the losses incurred. A major breakthrough was the amendment to the Information Technology Act of 2000 and enactment of the Information Technology (Amendment) Act, 2008 (**"IT Act"**), which was envisaged following the arrest of Avinash Bajaj, CEO, Baazi.com who was indicted for transmitting obscene pictures of schoolchildren. A need was felt to strengthen the data and privacy protection framework to cater to the fast growing IT industry.

2.0 Personal information recognized as "sensitive"

To satisfy the long-felt need for protecting confidential data and information handled by the outsourcing sector, the only legislative initiative that attempted to establish an elaborate data protection regime in India is the IT Act. The IT Act formally introduces the concept of data protection in Indian law, ushers in the concept of "sensitive personal information" and provides for fixation of liability on a body corporate to preserve and protect such sensitive personal information.[3] It further provides for civil and criminal liability for failure to protect personal data and information.[4] However, the IT Act, instead of tightening the noose on cyber crimes actually seeks to lessen the quantum of punishment and make most cyber crimes, barring a few, non–bailable. It goes without saying that the criminals, once set free, will use all their faculties and resources in wiping out all incriminating electronic trails and evidence. At a time when governments around the world have adopted the strictest policies to tackle cyber threats, this move of the legislature is adverse for the interest of the IT industry.

Nevertheless, the IT Act also makes provisions for legal action for individuals in cases of breach of confidentiality and privacy, under lawful contract.[5] The IT Act enables the government to lay down a uniform encryption policy for securing electronic communications, which was hitherto absent. Section 43A imposes the obligation to follow reasonable security practices and procedures on all businesses handling sensitive personal data or information. The parties are at liberty to identify the best security practices[6] and incorporate them in a binding agreement between them. In such agreements, parties can decide on the quantum of the penalty that may be imposed in the event of breach as there is no cap provided under section 43A. This contractual obligation will keep the Indian companies exposed to potential claims for damages that are not capped. Further, section 72A addresses issues emerging from

[3] Section 43A of the IT Act.
[4] Refer to sections 43A and 72A, newly introduced.
[5] Section 72A of the IT Act.
[6] The section also provides that the security practices can be specified either by Government of India coupled with the assistance of industry organizations or by any other law. So far, the Government has not notified any framework pursuant to the new section. Accordingly, the parties are free to agree on mutually acceptable terms regarding the security measures, including the applicable law.

data sabotage, and imposes punishment and fine for the person misusing the information with *mala fide* intent.

In order to define "sensitive personal data" with the help of professional bodies, the Department of Information Technology, Ministry of Communications and Information Technology sought views of Data Security Council of India (**"DSCI"**) and NASSCOM on making of Rules under sections 43A.[7] DSCI is a not-for-profit self-regulatory organization by the industry under the aegis of NASSCOM. DSCI has developed a "Best Practices Framework" based on ISO 27001 Security Standards and OECD Privacy Principles[8] to ensure compliance with international standards and to ensure that India remains a destination of choice for global consumers. The principal guidelines provided by DSCI are self regulation, adoption of best global practices, independent oversight, focused mission and enforcement mechanism. Given the emphasis that is being put on self mechanism in the IT industry, it may be worthwhile giving self regulation legal recognition. Involving members from the IT industry in the process to address the specific technological concerns may result in a more effective mechanism for data security management.

3.0 Need for coherent initiatives – Issues, suggestions & initiatives

Generally, the legal issues concerning data protection include e-commerce, encryption policy, cyber security and national security. Considering the significance attached to personal information, India is under a moral as well as legal obligation to enact privacy and data protection regulations, which can be done either by self-regulation or by a separate law. Any new data protection laws must address these issues specifically. Given the significance of data protection for Indian IT industry, India can attempt to inculcate principles enshrined in the global regulations- OECD,[9] European Union and APEC,[10] which are the major privacy principles that form the basis of many privacy laws throughout the world and are the most widely accepted.[11] The legislation must also work around bureaucratic impediments so as not to render it ineffective at operational level, and not to encumber business interest. The law should address significant issues relating to trespass upon individual privacy, including digital and electronic communications and prohibit the use of cutting-edge technology to trespass upon privacy rights and personal data.

Worried about the negative impact of the recent leakage of intercepted conversations, the government has started working on framing a privacy law, essentially by amending the Communications Convergence Bill 2001. The new law is expected to frame rules for monitoring phone and internet and for providing redressal mechanism in case of any breach of privacy. This proposed legislation on data protection will ensure confidentiality of all

[7] As available on < http://www.naavi.org/ita_2008/draft_rules_ita_2008/rules_draft_dsci.pdf> last accessed on December 23, 2010.
[8] Available on the official website of DSCI http://www.dsci.in/node/500 last visited on December 15, 2010.
[9]Organization for Economic Co-operation and Development. For details visit: http://www.oecd.org/ last visited on December 21, 2010. OECD Guidelines apply to Europe, North America and developed Asian nations.
[10] Asia-Pacific Economic Cooperation. For details visit http://www.apec.org/ last visited on December 21, 2010.
[11]Kamlesh Bajaj, (CEO, DSCI) 'Data Security Council of India- A self Regulatory Organization', available on http://www.dsci.in/taxonomypage/348 last visited on December 16, 2010.

information transmitted through computer networks and telephones. Communications Commission of India is also proposed which will be a regulator with wide powers to take up complaints by citizens on breach of privacy in the name of law enforcement. Under the prevailing laws, a "wrongly" wiretapped person has no real protection apart from filing a case for violation of fundamental right. Though this regulation is also expected to cover the data privacy of the IT industry, it will be too preliminary to comment as to how this will address to the privacy issues of the IT industry.

Conclusion

Though the IT Act has brought some solace to the IT sector, there are several grey areas in data protection and privacy that needs immediate address. It has to be borne in mind that although the data protection initiatives discussed above comprise a promising start, yet, there exists a dire need for further regulation and standardization to meet the demands of this fast growing industry. A legal framework needs to be established setting specific standards relating to the methods and purpose of assimilation of personal data and secure means of commerce. Consumers must be made aware of voluntarily sharing information and no data should be collected without express consent. In USA, for instance, there are 45 Federal enactments and about 598 State enactments that can be attributed to security and privacy. In UK, the Data Protection Act had made a foray in the legal realm as early as 1984, following the European Convention on Data Protection.[12] Keeping in view the international developments, it is incumbent upon the government and the industry, to work in unison and create a world class data protection regime in India, and thus do justice to the industry that has been giving the nation so much in terms of revenue, employment and GDP.

This E-Newsline is prepared by Anubhuti Pandey (under the supervision of Neeraj Dubey, Sr. Associate), a 4th year law student at Hidayatullah National Law University, Chhattisgarh who is pursuing her internship at PSA.

[12]David Bainbridge, Encyclopedia of Information Technology law- Data Protection Law, second ed, Universal Law Publishing Co, 2007 p. 4.