THE INDIAN JOURNAL OF LAW AND TECHNOLOGY
Volume 4, 2008

DATA PROTECTION EFFORTS IN INDIA: BLIND LEADING THE BLIND?

*Latha R. Nair**

ABSTRACT

This paper, after establishing the need for effective data protection in India, goes on to describe the rudimentary measures taken in the country till date in the sphere of data protection. While highlighting the inadequacy of such measures and the ambiguity in proposed amendments, the author seeks inspiration from European Union law in proposing a broad framework for data protection law in India.

TABLE OF CONTENTS

* Latha R. Nair is a partner at K&S Partners, New Delhi. She may be contacted at latha@knspartners.com.

I. WHY PROTECT DATA?

The need to protect data and data privacy in India is relatively new, arising from the ever expanding off-shoring business operations conducted in India by overseas companies wherein personal data is exported by these overseas companies to their off-shore agents or counterparts in India.[1] If it was not for this mushrooming off-shoring business, India would perhaps never have worried much about data protection, as there are already existing provisions in the Indian legal framework for protection of data, albeit not at the scale at which protection is warranted under the current circumstances.

Keeping in mind that data is the principal basis of most off-shoring businesses, it would be instructive to examine the intended objectives of any data protection law. For instance, the European Data Protection Directive[2] has as its twin objectives the protection of privacy of individuals with regard to the processing of personal data and, the facilitation of the free movement of such data. The two stated objectives would ordinarily contradict each other, and the task confronting any authority would be to reconcile these objectives by protecting privacy rights, while simultaneously ensuring the free movement of data.[3] In other words, the directive aims to achieve processing of data by maintaining data privacy.

India had been the hot-spot for off-shoring operations for foreign companies for a long time, till concerns of data security were raised, following certain incidents of data theft and breach of data privacy by certain Indian off-shoring

---

1 *See* Jürgen Schaaf and Thomas Meyer, *Outsourcing to India: Crouching Tiger Set to Pounce* (Deutsche Bank Research), Oct. 25, 2005, *available at* http://www.dbresearch.com/PROD/DBR_INTERNET_EN-PROD/PROD0000000000192125.pdf (stating that India is the world's most important offshoring location).

2 Council Directive 95/46, 1995 O.J. (L281) 31 (EC).

3 *See* CHRIS REED, COMPUTER LAW 418 (5th ed., 2004) (explaining how the Data Protection Directive mirrors the 1981 Council of Europe Convention on data protection which attempts to reconcile privacy and the desire to maintain free flow of information between trading nations).

companies.[4] These incidents made headlines in national and international media and brought India's legal framework for data protection under worldwide scrutiny. While India continues to be a hotspot for off-shoring, it cannot avoid data security issues for much longer, as both the industry and the government have been under tremendous pressure to enact a law for data protection in India.

II. EXISTING LEGAL FRAMEWORK FOR DATA PROTECTION IN INDIA

A. Contract Law

The existing Indian legal framework for data protection from an off-shoring angle falls mainly under the law of contract. Under the Indian Contract Act, 1872, a company can bind another through a contract to protect the data of the former. This is possible because of the reason that the Act defines 'consideration' as any act or abstention at the desire of the promisor,[5] which means that for certain reciprocal consideration, one firm can bind another so as to refrain from revealing data without authorisation, and foist upon it the positive obligation to protect data. Such a contract may mention the specific duties and obligations of both the parties involved and should have provisions relating to the duty of the Indian company to protect privacy of data, as well as the terms and conditions of the use and processing of data. Currently, all off-shoring operations in India are regulated by such contracts. In a scenario like this, contractual clauses are crucial in order to determine the extent of data security. Most of the time, negotiations by foreign data exporters with Indian companies aim at reaching a balance between maximum business benefits and adequate protection of personal data.

---

[4] *See, e.g., Ex-IITian Arrested for Delhi Call Centre Data Theft*, THE TIMES OF INDIA, Nov. 12, 2005, *available at* http://timesofindia.indiatimes.com/articleshow/1293310.cms.

[5] Section 2 of the Indian Contract Act states that "[w]hen, at the desire of the promisor, the promisee or any other person has done or abstained from doing, or does or abstains from doing, or promises to do or to abstain from doing, something, such act or abstinence or promise is called a consideration for the promise."

B. The Information Technology Act, 2000

Apart from the Indian Contract Act, 1872, some provisions pertaining to data protection are also present in the Information Technology Act, 2000. The Information Technology Act (hereinafter, "The IT Act") was enacted in 2000 with the main purpose of providing legal recognition to transactions carried out by means of electronic commerce, as has been stated in its preamble. The definition of 'data' in the Act covers a representation of information, knowledge, facts and so on, which are being prepared or processed in a computer system in any form or stored internally in the memory of the computer.[6]

Section 43(b) of the IT Act stipulates penalties by way of damages up to Rs. 10,000,000 against any person who "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".

Further, Section 66 of the Act defines 'hacking', and lists the punishment for the same. It reads:

> *66. (1) Whoever, with the intent to cause or knowing that he 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 with imprisonment up to three years, or with a fine which may extend up to two lakh rupees, or with both.*

The expression "or affects it injuriously by any means" could be interpreted to include a breach of privacy of the data. Hence, although the IT Act primarily provides legal recognition for transactions carried out by means of electronic commerce, there are some provisions dealing with data protection.

---

[6] Section 2 of the IT Act defines 'data' as "representation of information, knowledge, facts, concepts or instruction which are being prepared or have been prepared in a formalised 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".

III. RECENT EFFORTS IN INDIA TOWARDS DATA PROTECTION

Instances of data theft have compelled both the government and the industry to remedy the situation as a response to international pressure, in terms of providing some sort of framework for data protection. Some of these efforts are discussed below.

A. Proposed Amendments to The IT Act

In view of growing concerns raised by recent instances of data theft, the Ministry of Information Technology proposed certain amendments to the IT Act, 2000. One such amendment, pertinent to data protection, is the proposed insertion of a new Section 43A wherein sensitive personal information would be handled with reasonable security practices and procedures. The proposed amendment reads as follows:

> *43A. 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 not exceeding five crore rupees, to the person so affected.*
>
> *Explanation: — For the purposes of this section,—*
>
> *i) 'body corporate' means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;*
>
> *(ii) 'reasonable security practices and procedures' means security practices and procedures designed to protect such information from unauthorised 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;*

(iii) 'sensitive personal data or information' means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

This has taken the form of Clause 20 of the Information Technology (Amendment) Bill, 2006.

However, nothing in the proposed amendments deals with crucial aspects of data protection such as the processing of personal data, handling of sensitive personal data, the conditions under which data may be collected from an individual, the precautions to be taken while collecting data, confidentiality and security of processing of the data collected and so on.

The proposed amendments have not yet materialised into new provisions under The IT Act and have only recently received the comments of the Standing Committee on Parliamentary Affairs.

B. The Data Security Council of India

The National Association of Software and Services Companies (NASSCOM) has set up a self-regulatory initiative in data security and privacy protection called the Data Security Council of India (DSCI). What led to the establishment of the DSCI is the continuing effort by NASSCOM to ensure that the Indian information technology industry has a safe environment that can be benchmarked with the rest of the world.[7]

The DSCI is a self-regulatory body established under the premise that the industry, rather than the government, is best positioned to develop appropriate data privacy and security standards as it has greater knowledge and better understanding of the practical commercial issues involved. It is felt that such an approach would allow the DSCI to evolve and effectively respond to global developments. The DSCI would adopt global standards in order to move towards this end, initially focussing on establishing its membership and evolving a code of conduct by promoting a culture of privacy. Initially, the DSCI would promote

---

[7] *See* Data Security Council of India (DSCI), *available at* http://www.nasscom.in/Nasscom/templates/NormalPage.aspx?id=51973.

and encourage voluntary compliance with the code of conduct, gradually creating a mechanism for enforcement of the same in an effort to establish its credibility.[8]

The DSCI is envisaged as a non-profit organisation, with its governing body having an adequate representation of independent directors and industry specialists. Organisations associated with data security and privacy protection such as Information Technology (IT) and Information Technology enabled Services (ITeS) companies, academic or research institutions and universities can also become members of the DSCI.[9]

The DSCI's stated mission seeks to:[10]

- Enable IT and ITeS companies to provide a high standard of security and data protection by adopting best practices.
- Develop, monitor and enforce an appropriate security and data protection standard for the Indian IT and ITeS industry that would be adequate, cost effective, adaptable and comparable with global standards.
- Build capacity to provide security certification for organizations.
- Create a common platform to promote the sharing of knowledge about information security and foster a community of security professionals and firms.
- Create awareness among industry professionals and other stakeholders about security and privacy issues.

C. National Do Not Call Register

As discussed at the very outset, any data protection law should aim at protecting the privacy of data and, at the same time, ensuring the free movement of data. The issue of privacy of personal data, especially personal telephone

---

8 *See Data Security Council of India: A Self-Regulatory Initiative in Data Security and Privacy Protection, available at* http://www.nasscom.in/upload/5216/Datasecurity.pdf (setting out the objectives of the Council in the guiding principles).

9 *Id.*

10 *Id.*

numbers, has been the subject of great discussion among legal and industry circles in the recent past in India. The multiplicity of telecommunication service providers, coupled with easy and inexpensive mobile phone connectivity has led to rampant breaches of the personal privacy of mobile phone users. Taking advantage of the enormous amounts of freely available mobile phone user data, many industries in the finance, banking, health and tourism sectors have set up telemarketing services to tap the potential business opportunities that lie in such data. Consequently, telemarketing calls have become yet another intrusion introduced by the digital revolution in the lives of Indians, and what initially appeared to be a matter of routine inquiries regarding loans or credit card requirements turned out to be a massive and unabated nuisance to the receivers of such calls.

Eventually, the Telecom Regulatory Authority of India (TRAI) had to take steps to curb these unsolicited commercial calls pursuant to a petition filed by a Delhi-based lawyer before the Delhi State Consumer Dispute Redressal Commission (hereinafter "the Commission") against a leading private telecom company, Airtel, along with two banks, on various counts including breach of privacy, financial loss, mental harassment and agony, and wrongful gain by the respondents. While allowing the petition and passing severe strictures against the respondents, the Commission also directed the establishment of a National 'Do Not Call' Register by TRAI, which would bind all the players in the market, placing special emphasis on the fact that commercial telemarketers could not call a subscriber if their number was on this Register. On the establishment of such Register, subscribers would be called upon to register their telephone numbers free of cost through the Internet by publicising such a Register in the newspapers.[11]

Effective from October, 2007, TRAI put in place the National 'Do Not Call' Registry (NDNC), with the primary objective of curbing unsolicited commercial communication (UCC). The Telecom Unsolicited Commercial Communications Regulations, 2007, defines UCC as, "any message, through telecommunications service, which is transmitted for the purpose of informing about or soliciting or promoting any commercial transaction in relation to goods,

[11] *See Heavy Fines Imposed on Telemarketing Company*, http://news.indlaw.com/guest/databasesearch/articles/core_articledisplay.asp?ID=Unsolicited_focus2.

investments or services which a subscriber opts not to receive."[12] Exceptions to UCC are messages received under a contract, communications relating to charities etc., and communications transmitted under the directions of the government, in the interest of the sovereignty and integrity of India.

The NDNC register will, therefore, be a database containing the list of all telephone numbers of subscribers who do not wish to receive UCC.[13]

IV. DO THESE EFFORTS BY INDIA SUFFICE?

It is evident from the most recent steps taken by India toward data protection as listed above that there is a strong awareness and inclination on the part of the government and the industry to protect data in India. However, are these steps constructive enough to offer comprehensive protection for data as well as provide the required comfort level to foreign companies to engage in off-shoring business activities in India? Or are they mere baby steps taken in the direction of data protection? The following section aims at examining whether these would, in fact, provide adequate protection to the world's largest back office operations taking place in India.

A. Amending The IT Act to Protect Data: Fitting a Square Peg in a Round Hole?

Let us first look at the proposed amendments to The IT Act. A reading of the preamble to The IT Act indicates that it is an Act to provide legal recognition to transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as 'electronic commerce' transactions. The preamble does not mention data protection as an objective although one of the purported objectives of the proposed amendments to The IT Act is data protection. Since India's experiences from the inadequacy of data protection in these times of off-shoring are unprecedented and new, it would be useful to look at jurisdictions such as Europe which have existing e-commerce and data protection laws. The member

---

[12] Telecom Unsolicited Communications Regulations 2007, Regulation 2(q).

[13] *See* National Do Not Call Registry, *available at* http://ndncregistry.gov.in/ndncregistry/index.jsp.

countries of the European Union are also obligated to enact national laws for various areas, including that of data protection and e-commerce.[14]

As part of the harmonisation of the European Union, there are various directives that member countries are required to adopt as their national laws. Two such directives in the areas of data protection and e-commerce are, European Directive 95/46/EC (hereinafter, the "Data Protection Directive") and European Directive 2000/31/EC (hereinafter, the "E-commerce Directive"). The Data Protection Directive was enacted for the protection of individuals with regard to the processing of personal data and the free movement of such data.[15] On the other hand, the E-commerce Directive was enacted with a view to, *inter alia*, contribute to the proper functioning of the internal market by ensuring the free movement of information society services among the member states.[16]

Under Article 2(a) of the Data Protection Directive, 'personal data' is defined as, "any information relating to an identified or identifiable natural person." The Directive is to apply to the processing of personal data, wholly or partly by automatic means, and to the processing of personal data which forms part of a filing system, otherwise than by automatic means. Certain types of processing, such as the processing of personal data for public security, defence, state security, activities in the areas of criminal law and processing by a person in the course of personal or household activities, are exempt from the scope of the Directive.[17]

Under the Directive, member states are under various obligations, including ensuring that data is processed fairly and lawfully, that it is collected for specified and legitimate purposes and not processed in a manner incompatible with those purposes, that the processing of data is adequate, relevant and not excessive in relation to the purposes for which it is collected and/or further processed and that the data collected is accurate and kept up to date and kept in a form which

---

[14] For instance, the United Kingdom enacted the Data Protection Act in order to conform to EC Directive 95/46/EC, as is evident in the preamble of the Act.

[15] Council Directive 95/46, art.1, 1995 O.J. (L281) 31 (EC).

[16] Council Directive 2000/31, art.1, 2000 O.J. (L178) 8 (EC).

[17] *Supra* note 15, art. 3.

permits the identification of data subjects etc.[18] Further, personal data may be processed only if the data subject has unambiguously given his consent and such processing is necessary not only for the performance of a contract to which the data subject is party but also for the protection of the interests of the data subject.[19]

Besides, the Directive prohibits not only the processing of certain personal data (such as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, and health or sex life), but also processing for the purposes of preventive medicine, medical diagnosis, offences and criminal convictions, and so on, except under certain conditions.[20] Further, the data subject must be provided a right to object to the processing of data relating to him and, where there is a justified objection, it must be provided that the processing may no longer involve such data.[21] Apart from being under an obligation to keep the confidentiality of the processing of data,[22] the entity processing the data must also be required to implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction, accidental loss, unauthorised disclosure etc.[23]

These are some of the salient features of the Data Protection Directive. It is, therefore, evident that the Directive covers a whole range of issues associated with processing of personal data in keeping with the twin objectives of the Directive, as discussed earlier.

The E-commerce Directive specifically excludes from its purview, issues relating to information society services already covered by the Data Protection Directive.[24] Since its objective is to provide for certain legal aspects of information society services, in particular electronic commerce, the E-commerce Directive stipulates various requirements to be imposed on service providers by member

---

[18] *Id.* at art. 6.

[19] *Id.* at art. 7.

[20] *Id.* at art. 8.

[21] *Id.* at art. 14.

[22] *Id.* at art. 16.

[23] *Id.* at art. 17.

[24] *Supra* note 16, at art. 1(5) (b).

states and required to be complied with by service providers. The Directive requires a member state to ensure that service providers render information such as their names and addresses, along with their electronic mail addresses that allow contact and communication with them in a direct and effective manner, as also details of any public registration or identification number, and so on.[25] Further, it stipulates that commercial communications, which are part of an information society service, comply with certain conditions, such as ensuring that the communication as well as the person making the communication shall be clearly identifiable.[26] Under the Directive, UCC by electronic mail by a service provider established in their territory shall be identifiable, clearly and unambiguously, as such, as soon as it is received by the recipient.[27] Also, service providers undertaking UCC by electronic mail must regularly consult the opt-out registers in which persons not wishing to receive such commercial communications can register themselves.[28] The Directive also exempts intermediary service providers of liability in situations when they are mere conduits,[29] as also in cases of caching[30] and hosting,[31] and stipulates that member states are not to impose a general obligation to monitor the service providers.[32]

Hence, the E-commerce Directive covers issues raised in the context of information society services, service providers, and the obligations of member states and the providers of these services regarding such services.

An overview of both these directives reveals that while the E-commerce Directive deals with all aspects of information society services in detail, the Data Protection Directive deals in detail with one aspect of information society services, namely data protection. Also, while both these directives deal with aspects of information society services, the object and concept of both are distinct and different.

---

[25] *Id* at art. 5.

[26] *Id.* at art. 6.

[27] *Id.* at art. 7 (1).

[28] *Id.* at art. 7 (2).

[29] *Id.* at art. 12.

[30] *Id.* at art. 13.

[31] *Id.* at art. 14.

[32] *Id.* at art. 15.

As India is treading new ground as far as data protection and e-commerce laws are concerned, it would be useful to take a leaf or two out of Europe's experience in establishing a legal framework for data protection. While all data transfers and processing are e-commerce transactions, all e-commerce transactions are not data transfers or processing. This explains why the European E-commerce Directive specifically excludes from its purview issues relating to information society services which are already covered by the Data Protection Directive. Although data protection is part of e-commerce, the implications of protecting data have a wider reach and scope and will have to be dealt with in detail through a separate piece of legislation. By attempting to fit provisions for data protection into The IT Act, comprehensive data protection cannot be achieved. For instance, the proposed amendments would not ensure that data is processed fairly and lawfully, that it is collected for specified and legitimate purposes and not processed in a manner incompatible with those purposes, that the processing of data is adequate, relevant and not excessive in relation to the purposes for which it is collected and/or further processed or that the data collected is accurate and kept up to date and kept in a form which permits identification of data subjects, that the data subject has unambiguously given his consent in processing data, that adequate measures are taken to ensure data privacy etc.[33]

In fact, such issues arising out of data protection are relevant not only to the off-shoring industry, but also to domestic IT-savvy industries and operations in India. For instance, a recent move by the state of Karnataka, stipulating biometric identification through fingerprints for ration card holders, came in for a lot of criticism from certain activists, who argued that such an extensive database, in the absence of a data protection law, would be intrusive and vulnerable to misuse.[34] Perhaps, the off-shoring business has paved the way for a sort of new awakening to issues of privacy in a country like India, where notions of personal privacy are brushed aside in a cultural milieu of sharing and accommodating.

---

[33] In other words, the proposed amendments would not achieve the wider ends enshrined in the eight data protection principle contained in Article 6 of the Data Protection Directive.

[34] *See* Bageshree S., *Now Biometric Identification for Ration Cards Too*, THE HINDU, Nov. 29, 2007, *available at* www.hindu.com/2007/11/29/stories/2007112954530500.htm.

In this connection, it is also relevant to mention the report of the Standing Committee on Information Technology on the proposed amendments to the IT Act, as well as the recommendations made by it. The Information Technology (Amendment) Bill, 2006 was introduced in Parliament on 15th December, 2006, and referred to the Standing Committee on Information Technology on 19th December, 2006 for examination. On 29th August, 2007, the Committee considered and adopted a Draft Report. It appears from the report that, while there were suggestions for separate data protection legislation from the industry and the Department of Information Technology, there was perhaps not enough consensus, conviction or understanding on the need for the same.[35]

B. DSCI and NDNC

While the efforts made by NASSCOM in establishing the DSCI are commendable, only time would tell whether the self-regulation of an industry of this sort is a lotus-eater's vision or an achievable dream. The DSCI's stated mission is extremely encouraging in these times, when data security is one of the major concerns for foreign investors in India. The DSCI would have to build up a sufficient membership, with the willingness to comply with its code of conduct, before it can push forward its stated objectives. If and when a data protection law is enacted by India, the DSCI could play a pivotal role in administering such a law. While it is too early to comment on how effective the DSCI is in data protection, it certainly is a positive step in that direction.

The effect of the establishment of the National 'Do Not Call' Register on telemarketing calls has been quite dramatic, in that there has been a remarkable slide in the number of calls to those who took the effort to opt out by registering in the register under the NDNC. Also, as in the case of the DSCI, it is too early in the day to comment on the NDNC's functioning or its efforts to protect data privacy.

---

[35] *See* STANDING COMMITTEE ON INFORMATION TECHNOLOGY, TENTH REPORT, *available at* http://164.100.24.208/ls/CommitteeR/Communication/10rep.pdf.

V. A CASE OF THE BLIND LEADING THE BLIND OR OF TURNING A BLIND EYE?

All the above Indian endeavors towards data protection, though with the best of intentions, could perhaps be described as a case of the blind leading the blind. Or is it a case of the powers-that-be turning a blind eye to the issue? A reading of the report of the Standing Committee on Information Technology on the proposed amendments to The IT Act concerning data protection makes it clear that while the industry and the legislators are familiar with terms like 'personal data', 'sensitive personal data', 'personal privacy', 'data privacy' and so on, there is a lot of ambiguity as to how these terms should be interpreted for effective data protection in India.[36] Without an in-depth understanding of the industry's needs and what is involved in the protection of data and data privacy in India, all the above efforts will remain mere efforts. Nor would attempts to do patchwork on existing legislation, so as to protect data, meet the current need for a legal framework. Emulating the European example of data protection by distinguishing it from protection of e-commerce transactions would undoubtedly place India on the global map when it comes to data protection. Besides, it would also create a safe environment for foreign companies to invest in India. Till then, it needs to be seen how long the off-shoring industry is going to indulge India's baby steps towards data protection.

[36] *Id.*