

## **NOTE ON DATA PROTECT**

### **Introduction**

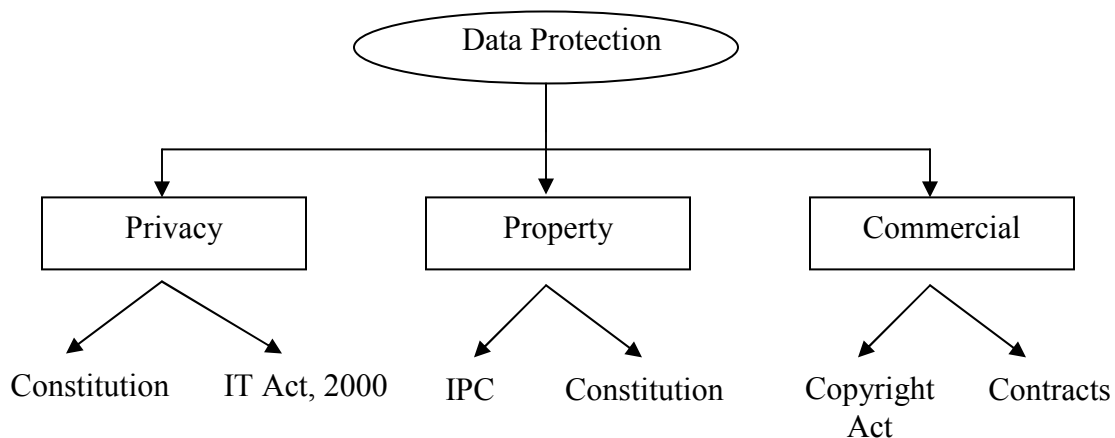
Recently, the call-center industry was taken aback without warning when the Economic Offences Wing (EOW) of the Delhi police arrested four employees of a call centre for having allegedly stolen data from M/s Parsec Technologies Limited (PTL), the company they were employed in. The accused had sold the stolen data to clients in the United States through a parallel company M/s Telequest Systems (of which one of the partners had been team leader for data management with PTL since November 2001 until he left the company a few months before the loss was discovered).

The gravity of the issue of data protection was brought to light yet again when one of the leading corporate law firms, Titus and Co., filed an FIR against some of its associate lawyers alleging criminal breach of trust and theft of electronic records.

The above two incidents serve as a grim reminder of the stark inadequacy of data security mechanisms in India, unlike in the US (the ‘Safe Harbor’ principles, 2000), the UK (Data Protection Act, 1998), and the EU (Directive on Data Protection, 1998) where the most stringent of norms have been formulated. This update therefore seeks to identify the existing laws that could be applied towards data protection in the absence of any current legislation on the matter.

### **Existing legal framework**

Data protection can be said to involve three connected although different aspects.



## Constitution

The Constitution of India (“Constitution”) makes no specific mention of privacy, but the courts have implicitly read such a right into Article 21 and Article 19(1)(d) (*Kharak Singh v. State of UP, AIR 1963 SC 1295* followed subsequently again in *People’s Union for Civil Liberties v. Union of India, (1997) 1 SCC 301*). The right to privacy can also be derived from other statutes. For instance, the Public Financial Institutions Act of 1993 can be argued to be the source of the norm of confidentiality in bank transactions. Consequently, its breach can be used to build up an argument of violation of privacy as read into the Constitution. An argument<sup>1</sup> has also been made under the Constitution on the basis of Article 300A, which is the source of the right against deprivation of property except by authority of law. This however may not be a successful alternative since firstly, these rights can be claimed only as against the State and do not cover private employer-employee relationships. Second, the data should be proven to be ‘property’.

## The Information Technology Act, 2000

The Information Technology Act, 2000 (“IT Act”) prescribes punishment for ‘cyber contraventions’ (Section 43 (a) to (h)) and ‘cyber offences’ (Sections 65-74). The former would include gaining unauthorized access, and downloading or extracting data stored in computer systems or networks, and may result in civil prosecution. The latter category covers ‘serious’ offences like tampering with computer source code, hacking with intent to cause damage, and breach of confidentiality and privacy, all of which would invite criminal prosecution. Any person who has secured unauthorized access to a computer system or network, or has extracted any data<sup>2</sup>, or tampered with it in any way, is liable to compensate a person suffering damage thereby for an amount that can extend to INR 10,000,000.<sup>3</sup> The IT Act penalizes hacking,<sup>4</sup> as also the act of tampering with the computer’s source code<sup>5</sup> by providing for imprisonment up to 3 years or fine up to INR 200,000 or both. Further, if a person having powers under the IT Act,

<sup>1</sup> Pravin Dalal, Cyber-law India

<sup>2</sup> “Data” means representation of information, knowledge etc, prepared in a formalized manner, and intended to be processed. It can be stored in any form, whether in the internal memory or in punched cards, tapes, printouts, or optical storage media (Section 2(o) of the IT Act).

<sup>3</sup> IT Act, Section 43

<sup>4</sup> IT Act, Section 66

<sup>5</sup> IT Act, Section 65

breaches confidentiality and privacy by disclosing the data to another, he is punishable with 2 years imprisonment or fine up to INR 100,000 or both.<sup>6</sup>

In all such cases of offences or contraventions, the ‘network service provider’ or the ‘intermediary’, can also be made liable for any 3<sup>rd</sup> party information or data made available by him if it was done with his knowledge or if he did not exercise due diligence to prevent the offence.<sup>7</sup> ‘Intermediary’ is defined to mean anybody who receives, stores or transmits a particular electronic message on behalf of another person, or who provides any service with respect to that message.<sup>8</sup> Therefore a BPO can be made liable as a ‘network service provider’ since it is acting as a service provider making available information or data. The precedent was set in 2004 when the police arrested Bazeem.com’s CEO for making available scandalous material on his portal. The IT Act covers offences and contraventions committed abroad as well, irrespective of the nationality of the person, as long as the computer system or network is located in India.<sup>9</sup>

### **The Indian Penal Code, 1860**

The Indian Penal Code, 1860 (“IPC”) can be used as an effective means to criminalize data theft. The prosecution can proceed for misappropriation of property, theft, or criminal breach of trust. The offences of theft<sup>10</sup> and misappropriation<sup>11</sup> under the IPC are punishable with imprisonment up to three and two years respectively, with or without fine. If a servant or clerk has committed theft of any property belonging to his master, he is punishable with fine and imprisonment up to 7 years.<sup>12</sup> Further, a person is said to have committed criminal breach of trust if he has misappropriated property from another with whom he is in a fiduciary relationship with. In case the offender is a clerk or servant, he is punishable with fine and imprisonment up to 7 years.<sup>13</sup> If he is a public servant, banker, merchant or agent, then he is punishable with fine and

---

<sup>6</sup> IT Act, Section 72

<sup>7</sup> IT Act, Section 79

<sup>8</sup> IT Act, Section 2(1)(w)

<sup>9</sup> IT Act, Section 75

<sup>10</sup> IPC, Sections 378, 379.

<sup>11</sup> IPC, Section 403

<sup>12</sup> IPC, Section 381

<sup>13</sup> IPC, Section 408

imprisonment up to 10 years.<sup>14</sup> In all other cases of criminal breach of trust, the accused is punishable with fine and/or imprisonment up to 3 years.<sup>15</sup>

### **The Copyright Act, 1957**

The Copyright Act, 1957 is the Indian legislation governing intellectual property rights in literary, dramatic, musical, artistic and cinematographic works. It has granted the status of “literary work” to databases as well, although this is limited only to computer databases. Therefore copying the computer database, or copying and distributing the database would amount to infringement of copyright in the same, giving rise to the remedy of injunction and damages for the plaintiff. A person who knows of such infringement and conceals it or abets it is also liable to pay fine up to INR 200,000 or imprisonment up to 3 years or both.

### **Others**

Besides the above legislation, business entities mostly try to seek protection under general contract law, by incorporating confidentiality clauses in their employment contracts etc. This however is not too satisfactory an option, since relying on contract law to protect data could turn out to be problematic, time consuming and perhaps even self-defeating. The need for statutory protection therefore is evident.

In the absence of any black-letter law on the matter, Indian Business Process Outsourcing (“BPO”) companies have implemented self-regulatory processes such as the BS 7799 and the ISO 17799. These are essentially standards for information security management, which restrict the quantity of data that can be made available to employees of BPO and call centres. Indian BPO outfits are also trying to deal with the issue by attempting to adhere to major US and European regulations. Most Tier I BPO companies today have certifications that comply with regulations like the Sarbanes Oxley Act, Safe Harbor Act, GLBA (Gramm Leach Bliley Act) for financial services, FDCPA (Fair Debt Collection Practices Act) for banking and HIPAA (Healthcare Insurance Portability and Accountability Act) for healthcare. While most laws and certifications are oriented around verticals, there are laws like the UK Data Protection (DPA) Act and the Sarbanes Oxley Act, which are laws for data security across different industries.

---

<sup>14</sup> IPC, Section 409

<sup>15</sup> IPC, Section 405

## Issues

In regard to the Constitution, an action based on the ground of privacy has limited scope, since rights derived from the Constitution can be claimed only as against 'State' or State enterprises and not private individuals.

Further, under the IPC, the crimes of theft and misappropriation can be only of 'movable property'. 'Movable property' has been defined to include corporeal property of 'every description' except land and things permanently attached to the earth (Section 22). Therefore, whether or not an action would lie under the IPC would depend upon whether the data in question is 'property' or not. First, it can be argued that the definition of 'movable property' must be interpreted widely. The use of the phrase 'every description' followed by exclusionary items like land etc. in Section 22 indicates that the definition was intended to be wide save for the exceptions specifically provided for. Therefore computer databases also, which are movable by their very nature, should be brought within the scope of the term. Second, it may be also argued that it is a form of intellectual property since the Copyright Act has explicitly provided protection to computer databases as 'literary work'.

Under the IT Act, the confidentiality obligations are limited to officers or persons having powers under the Act and does not extend to private persons. Further, the officer is not liable to compensate the person damaged by the disclosure. The Act must be amended to provide for such compensation. Moreover, most of the penalties are in the range of INR 200,000 to INR 500,000. They are very insignificant compared to the gains that a person may make out of the crime.

As far as the Copyright Act is concerned, difficulty may arise due to the difference that can be drawn between *data* protection and *database* protection. Data protection is aimed at protecting the informational privacy of individuals, while database protection has an entirely different function, namely the protection of the creativity and investment put into the compiling, verification and presentation of databases.<sup>16</sup> As far as database is concerned, Section 2(o) of the Copyright Act protects computer databases. The word 'database' is however not defined in the

---

<sup>16</sup> Simon Chalton, Change in Law Strengthens Database Protection, [1998] PLBIN 11 (Privacy Laws and Business International Newsletter), available at <http://www.worldlii.org/int/journals/PLBIN/1998/11.html>

Act. The IT Act has defined it to mean a ‘representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalized manner, or have been produced by a computer, computer system or network, and are intended for use’ in the same (Section 43- Explanation ii).

As regards copyright protection for other kinds of data/databases, the issue remains as regards the standards to be met for enjoying copyright protection. It is doubtful as to whether Indian copyright law would protect all data. The Burlington case followed the “sweat of the brow” doctrine laid down in *Govindan v. Gopalakrishna* (AIR 1955 Madras 39) wherein the work would be protected if the author has expended time, money, labour and skill on it (*Burlington Home Shopping Pvt. Ltd v. Rajnish Chibber & Anr*, 1995 PTC (15) 278). The Burlington case, applying the above ratio, held that a compilation of addresses was protected. Further, in *Himalaya Drug Co. v. Sumit* (Suit no 1719 of 2000), the Delhi High granted an injunction against an Italian, preventing him from copying the plaintiff’s online herbal database onto its own website. However, in *Eastern Book Co. v. Navin J. Desai* (MANU/DE/0066/2001), the court raised the standard to a ‘modicum of creativity’, which was originally laid down in the Feist case (*Feist Publications, Inc. v. Rural Telephone Service Company*, 499 U.S. 340 (1991)). Therefore the database sought to be protected must not only be an original creation, but it must also satisfy a minimum level of creativity.

### **The path ahead**

The government has proposed several amendments to the IT Act, which are to be implemented soon. The proposed amendment to Section 43 (unauthorized access) widens the ambit of persons liable for breach of data protection, by expressly providing that a body corporate dealing with sensitive personal information shall be liable to compensate a person suffering damage, due to such body corporate’s negligence in handling sensitive personal information. The parties are permitted to specify reasonable security practices contractually. In the absence of any contract to this effect, the reasonable security practice shall be determined by rules made by central government in consultation with the self-regulatory bodies. Further, the amendment proposes to replace “hacking” with a broader set of activities described as “computer related offences”, and provides for compensation to a person suffering loss thereby. As regards breach of confidentiality and privacy, the proposed amendments qualify such liability by providing that such person will be liable only if the disclosure is intentional. Therefore, an officer

who negligently discloses any information or material will not be liable to any punishment.

It is proposed to amend the Section 72 to provide that an intermediary shall be liable for breach of confidentiality only if the offence has been committed intentionally and with intent to cause injury to the subscriber. This would limit the liability of an intermediary significantly, as the intent to cause injury may be extremely difficult to prove or at times may not be intended at all. Further, Section 72 limits the compensation payable by the intermediary on breach to INR 2,500,000. This would conflict with the proposed amendment to Section 43. Under the amendable Section 43, compensation for negligence is INR 10,000,000, which is much more than compensation payable by an intermediary for intentional breach of privacy or confidentiality. Therefore, an intermediary may contend that the offence has been committed intentionally, and hence, the maximum amount of compensation cannot exceed INR 2,500,000. The sections must be harmonised to avoid conflict and misuse.

India is also planning to set up a 'Common Criterion Lab', backed by the Information Security Technical Development Council (ISTDC), where intensive research in cryptography and product security would be undertaken.

## **Conclusion**

Along with IT, comes greater accessibility of information, and when the employees, customers, and registered suppliers are able to interact electronically and remotely from any location, the risks to corruption only increase. The average cost of a data theft attack is Rs. 1.8 lakh, with the cost ranging between Rs. 20,000 and Rs. 1.87 crore, and two-thirds of data theft incidents are attributable to employees (current as well as former).<sup>17</sup> The Computer Crime and Abuse Report of 2001-2002 (India), indicated that the major categories of misappropriated data included source and object code (37%), credit card information belonging to the organization's employees and customers (29%), business related plans (20%) and other confidential information (14%).

The need for a law on data protection can therefore hardly be underemphasized if India has to sustain investor confidence especially amongst those foreign entities who send large amounts of data to India for back-office operations. This is all the

---

<sup>17</sup> Computer Crime & Abuse Report (India) 2001-02

more so, given the fact that many outsourcing arrangements involve entrusting an Indian company with a foreign company's confidential trade secret information, and/or its' customers' confidential data. It is hence critical that Indian laws provide a way to prosecute (and effectively deter) misuse of that information.

The Government of India, with the help of the Department of Information Technology, is currently working on a 'holistic law' on data protection. The proposed legislation will not just ensure data protection, but would also pave the way for appointment of a regulator to monitor the collected data and its usage. However, the law is yet to see the light of day. Until then, one can only wait.