

## White Paper on Privacy Protection in India

- Vakul Sharma

### 1.0 Introduction

Privacy as a concept involves what privacy entails and how it is to be valued. Privacy as a right involves the extent to which privacy is (and should be legally protected). “ The law does not determine what privacy is, but only what situations of privacy will be afforded legal protection<sup>1</sup>.” It is interesting to note that the common law does not know a general right of privacy and the Indian Parliament has so far been reluctant to enact one.

### 1.1 The Indian Perspective on Privacy

Competence of Central and State legislatures to enact legislations is derived from the Indian Constitution. The Seventh Schedule of the Constitution of India has three Lists, which contain various entries, which can be subject matters of legislation.

List I : Union List

List II : State List

List III : Concurrent List

The power to enact legislations on various subject matters listed therein comes from the following Articles of the Constitution of India:

Article 246 (1) of the Constitution of India gives the Parliament the exclusive power to make laws with respect to any of the matters enumerated in **List I** in the Seventh Schedule (Union List). This power of Parliament is unfettered by Article 246(2) and (3).

Article 246 (2) of the Constitution of India gives the Parliament and the State Legislature the power to make laws with respect to any of the matters enumerated in **List III** in the Seventh Schedule (Concurrent List). The power of the State Legislature is subject to Article 246(1) while the power of Parliament is unfettered by Article 246(3).

Article 246 (3) of the Constitution of India gives the State Legislature the exclusive power to make laws with respect to any of the matters enumerated in **List II** in the Seventh Schedule (State List). This power of the State Legislature is subject to Article 246(1) and (2).

---

<sup>1</sup> Hyman Gross, The Concept of Privacy, 42 N.Y.U.L. Rev. 36, 36 (1967).

“Privacy” is not a subject in any of the three lists in Schedule VII of the Constitution of India. But Entry 97 of List I states: “any other matter not enumerated in List II and List III .....” Thus only the Indian Parliament is competent to legislate on privacy since it can be interpreted as any other matter not enumerated in List II and List III.

Till date there is no specific enactment on Privacy. But the Constitution of India has embodied many Rights in Part III, which are called Fundamental Rights. These are enumerated in Article 14-30 of the Constitution.

Article 13 (2) prohibits the Indian State (Parliament and State legislatures) from making any law, which takes away or abridges the rights conferred by Part III.

Article 32 guarantees the right to move the Supreme Court of India for enforcement of the rights conferred by Part III.

This right is available against the State, which is defined in Article 12 as inclusive of the Government and Parliament of India and Government and Legislatures of each State and all local and other authorities in India.

From the above discussion it follows that while no legislative competence is found for the subject of Privacy, yet the Constitution of India has provided for many Rights (Fundamental Rights), which cannot be taken away by the State and are legally enforceable against the State.

## 1.2 Judicial Activism: The Right to Privacy

At this point begins the role of the Judiciary. Judicial activism has brought the Right to Privacy within the realm of Fundamental Rights. Article 141 of the Constitution states that “the law declared by the Supreme Court shall be binding on all courts within the territory of India.” Therefore, the decisions of The Supreme Court of India become the Law of the Land.

The Supreme Court of India has come to the rescue of common citizen, time and again by construing “right to privacy” as a part of the Fundamental Right to “protection of life and personal liberty” under Article 21 of the Constitution, which states “no person shall be deprived of his life or personal liberty except according to procedures established by law”. In the context of personal liberty, the Supreme Court has observed “those who feel called upon to deprive other persons of their personal liberty in the discharge of what they conceive to be their duty must strictly and scrupulously observe the forms and rules of the law”.

Even the fundamental right “to freedom of speech and expression” as enumerated in Article 19(1)(a) of the Constitution of India comes with reasonable restrictions imposed by the State relating to (i) defamation; (ii) contempt of court; (iii) decency or morality; (iv) security of the State; (v) friendly relations with foreign states; (vi) incitement to an offence; (vii) public order; (viii) maintenance of the sovereignty and integrity of India. Thus, the right to privacy is limited against defamation, decency or morality.

The Supreme Court has reiterated the Right to Privacy in the following cases:

1. *Kharak Singh v. State of UP*<sup>2</sup> In this case the appellant was being harassed by police under Regulation 236(b) of UP Police Regulation, which permits domiciliary visits at night. The Supreme Court held that the Regulation 236 is unconstitutional and violative of Article 21. It concluded that the Article 21 of the Constitution includes “right to privacy” as a part of the right to “protection of life and personal liberty”. The Court equated ‘personal liberty’ with ‘privacy’, and observed, that “the concept of liberty in Article 21 was comprehensive enough to include privacy and that a person’s house, where he lives with his family is his ‘castle’ and that nothing is more deleterious to a man’s physical happiness and health than a calculated interference with his privacy”.

2. *Gobind v. State of M.P.*<sup>3</sup> is another case on domiciliary visits. The Supreme Court laid down that “.....privacy-dignity claims deserve to be examined with care and to be denied only when an important countervailing interest is shown to be superior. If the Court does find that a claimed right is entitled to protection as a fundamental privacy right, a law infringing it must satisfy the compelling State interest test.....”

3. *State v. Charulata Joshi*<sup>4</sup> the Supreme Court held that “the constitutional right to freedom of speech and expression conferred by Article 19(1)(a) of the Constitution which includes the freedom of the press is not an absolute right. The press must first obtain the willingness of the person sought to be interviewed and no court can pass any order if the person to be interviewed expresses his unwillingness”.

---

<sup>2</sup> (AIR 1963 SC 1295)

<sup>3</sup> (1975) 2 SCC 148

<sup>4</sup> (1999) 4 SCC 65.

4. *R. Rajagopal v. State of Tamil Nadu*<sup>5</sup> The Supreme Court held that the petitioners have a right to publish what they allege to be the life-story/autobiography of Auto Shankar insofar as it appears from the public records, even without his consent or authorization. But if they go beyond that and publish his life story, they may be invading his right to privacy, then they will be liable for the consequences in accordance with law. Similarly, the State or its officials cannot prevent or restraint the said publication. It stated that “A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, child bearing and education among other matters.

None can publish anything concerning the above matters without his consent- whether truthful or otherwise and whether laudatory or critical. If he does so, he would be violating the right to privacy of the person concerned and would be liable in an action for damages.....”

5. *People’s Union for Civil Liberties (PUCL) v. Union of India*<sup>6</sup>, the Supreme Court held that the telephone tapping by Government under S. 5(2) of Telegraph Act, 1885 amounts infraction of Article 21 of the Constitution of India. Right to privacy is a part of the right to “life” and “personal liberty” enshrined under Article 21 of the Constitution. The said right cannot be curtailed “except according to procedure established by law”.

6. In *Mr. ‘X’ v. Hospital ‘Z’*<sup>7</sup> for the first time the Supreme Court articulated on sensitive data related to health. In this case, the appellant’s blood test was conducted at the respondent’s hospital and he was found to be HIV (+). His marriage, which was already settled, was called off after this revelation. Several persons including the members of his family and those belonging to their community came to know of his HIV (+) status and was ostracized by the community. He approached the National Commission against the respondent hospital claiming damages from them for disclosing information about his health, which, by norms of ethics, according to him, ought to have been kept confidential. The National Commission summarily dismissed his complaint. Consequently he moved the Supreme Court by way of an appeal.

---

<sup>5</sup> AIR 1995 SC 264

<sup>6</sup> (1997) 1 SCC 301

<sup>7</sup> (1998) 8 SCC 296)

The appellant argued that the principle of ‘duty of care’ as applicable to persons in medical profession also included the duty to maintain confidentiality and that since this duty was violated by the respondents, they were liable to pay damages. “Right of privacy may, apart from contract, also arise out of a particular specific relationship, which may be commercial, matrimonial, or even political. Doctor-patient relationship, though basically commercial, is professionally, a matter of confidence and, therefore, doctors are morally and ethically bound to maintain confidentiality.” It however, held that although it was the basic principle of jurisprudence that ‘every Right has a correlative Duty and every Duty has a correlative Right’, the rule was not absolute and was ‘subject to certain exceptions’ in the sense that ‘a person may have a Right, but there may not be correlative Duty, and the instant case fell within exceptions.

The court observed that even the Code of Medical Ethics carved out an exception to the rule of confidentiality and permitted the disclosure in certain circumstances ‘under which public interest would override the duty of confidentiality’ particularly where there is ‘an immediate or future health risk to others’. According to the court, the ‘right to confidentiality, if any, vested in the appellant was not enforceable in the present situation, as the proposed marriage carried with it the health risk from being infected with the communicable disease from which the appellant suffered.

As regards the argument of the appellant that his right to privacy had been infringed by the respondents by disclosing that he was HIV (+) and, therefore, they were liable in damages, the Supreme Court observed that as one of the basic human rights, the right of privacy was not treated as absolute and was ‘subject to such action as may be lawfully taken for the prevention of crime or disorder or protection of health or morals or protection of rights and freedom of others.’”

7. *District Registrar and Collector v. Canara Bank*<sup>8</sup>, it was held, that “exclusion of illegitimate intrusions into privacy depends on the nature of the right being asserted and the way in which it is brought into play; it is at this point that the context becomes crucial, to inform substantive judgment. If these factors are relevant for defining the right to privacy, they are quite relevant whenever there is invasion of that right by way of searches and seizures at the instance of the State.”

---

<sup>8</sup> (2005) 1 SCC 496: AIR 2005 SC 186

If one follows the judgments given by the Hon'ble Supreme Court, *three* themes emerge<sup>9</sup>:

- (1) that the individual's right to privacy exists and any unlawful invasion of privacy would make the 'offender' liable for the consequences in accordance with law;
- (2) that there is constitutional recognition given to the right of privacy which protects personal privacy against unlawful governmental invasion;
- (3) that the person's "right to be let alone" is not an absolute right and may be lawfully restricted for the prevention of crime, disorder or protection of health or morals or protection of rights and freedom of others;

### 1.3 Privacy and Data Protection

Privacy is closely connected to Data Protection. An individual's data like his name address, telephone numbers, profession, family, choices, etc. are often available at various places like schools, colleges, banks, directories, surveys and on various web sites. Passing on such information to interested parties can lead to intrusion in privacy like incessant marketing calls.

It would be a misnomer to say that India does not have 'data protection' legislation at all. This is factually wrong. The fact is that there exists data protection legislation in India. The subject matter of data protection and privacy has been dealt within the Information Technology Act, 2000 but not in an exclusive manner.

Data protection is not a subject in any of the three lists in Schedule VII of the Constitution of India. But Entry 97 of List 1 states: "any other matter not enumerated in List II and List III ....." Thus only the Indian Parliament is competent to legislate on data protection since it can be interpreted as any other matter not enumerated in List II and List III.

Data protection is, thus, a Central subject and only the Central Government is competent to frame legislations on issues dealing with data protection. In fact, the Information Technology Act, 2000, enacted by the Indian Parliament is the first legislation, which contains provisions on data protection.

---

<sup>9</sup> Sharma, Vakul. *Information Technology-Law & Practice*. Delhi: Universal Law Publishing Co. Pvt. Ltd, 2004.

### **1.3.1 The Information Technology Act, 2000**

The Indian Parliament enacted an Act called the Information Technology Act, 2000. It received the assent of the President on the 9<sup>th</sup> June, 2000 and is effective from 17<sup>th</sup> October, 2000. This Act is based on the Resolution A/RES/51/162 adopted by the General Assembly of the United Nations on 30<sup>th</sup> January, 1997 regarding the Model Law on Electronic Commerce earlier adopted by the United Nations Commission on International Trade Law (UNCITRAL) in its twenty-ninth session.

The aforesaid resolution of the U.N. General Assembly *recommends* that all States give favourable consideration to the Model Law on Electronic Commerce when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information.

It was a foresight on the part of the Government of India to initiate the entire process of enacting India's first ever information technology legislation in the year 1997 itself.

There were three reasons:

- (a) to facilitate the development of a secure regulatory environment for electronic commerce by providing a legal infrastructure governing electronic contracting, security and integrity of electronic transactions;
- (b) to enable the use of digital signatures in authentication of electronic records; and
- (c) to showcase India's growing IT prowess and the role of Government in safeguarding and promoting IT sector and attracting FDI in the said sector.

It is important to understand that while enacting the Information Technology Act, 2000, the legislative intent has been not to ignore the national or municipal (local) perspectives of information technology and also to ensure that it should have an international perspective as advocated by the UNCITRAL Model Law on Electronic Commerce.

### **1.3.2 Enumeration of the main principles of the Information Technology Act, 2000**

It is significant to note that by enactment of the Information Technology Act, 2000, the Indian Parliament provided a new legal idiom to data protection and privacy. The main principles on data protection and privacy enumerated under the Information Technology Act, 2000 are:

- (i) defining 'data', 'computer database', 'information', 'electronic form', 'originator', 'addressee' etc.
- (ii) creating civil liability if any person accesses or secures access to computer, computer system or computer network
- (iii) creating criminal liability if any person accesses or secures access to computer, computer system or computer network
- (iv) declaring any computer, computer system or computer network as a protected system
- (v) imposing penalty for breach of confidentiality and privacy
- (vi) setting up of hierarchy of regulatory authorities, namely adjudicating officers, the Cyber Regulations Appellate Tribunal etc.

Further, the Information Technology Act, 2000 defines certain key terms with respect to data protection, like access [S.2 (1)(a)], Computer [S.2 (1)(i)], Computer network [S.2 (1)(j)], Computer resource [S.2 (1)(k)], Computer system [S.2 (1)(l)], Computer database [S.43, *Explanation* (ii)], Data [S.2 (1)(o)], Electronic form [S.2 (1)(r)], Electronic record [S.2 (1)(t)], Information [S.2 (1)(v)], Intermediary [S.2 (1)(w)], Secure system [S.2 (1)(ze)] and Security procedure [S.2 (1)(zf)].

### **1.3.2.1 The Information Technology Act, 2000 provides for civil liability in case of data, computer database theft, privacy violation etc.**

The Act provides a complete Chapter (Chapter IX) on cyber contraventions, i.e., section 43 (a) – (h) which cover a wide range of cyber contraventions related to unauthorised access to computer, computer system, computer network or resources.

Section 43 of the Act covers instances such as: (a) computer trespass, violation of privacy etc. (b) unauthorised digital copying, downloading and extraction of data, computer database or information; theft of data held or stored in any media, (c) unauthorised transmission of data or programme residing within a computer, computer system or computer network (cookies, spyware, GUID or digital profiling are not legally permissible), (d) data loss, data corruption etc., (e) computer data/database disruption, spamming etc., (f) denial of service attacks, data theft, fraud, forgery etc., (g) unauthorised access to computer data/computer databases and (h) instances of data theft (passwords, login IDs) etc.

### **1.3.2.2 The Information Technology Act, 2000 provides for criminal liability in case of data, computer database theft, privacy violation etc.**

The Act also provides a complete Chapter (Chapter XI) on cyber offences, i.e., sections 65-74 which cover a wide range of cyber offences, including offences related to unauthorised alteration, deletion, addition, modification, alteration, destruction, duplication or transmission of data, and computer database.

For example, section 65 [Tampering with computer source documents] of the Act is not limited to protecting computer source code only, but it also safeguards data and computer databases; and similarly section 66 [Hacking with Computer System] covers cyber offences related to (a) Illegal access, (b) Illegal interception, (c) Data interference, (d) System interference, (e) Misuse of devices, etc.

Interestingly, section 72 [Penalty for breach of confidentiality and privacy] is aimed at public (and private) authorities<sup>10</sup>, which have been granted power under the Act to secure access to any electronic record, book, register, correspondence, information, document or other material information. The idea behind the aforesaid section is that the person who has secured access to any such information shall not take unfair advantage of it by disclosing it to the third party without obtaining the consent of the disclosing party.

### **1.3.2.3 Proposed amendments to the Information Technology Act, 2000 vis-à-vis data protection and privacy**

The Expert Panel constituted by the Department of Information Technology, Ministry of Information Technology, Government of India in its recommendations<sup>11</sup> proposed following amendments in the Act to strengthen data protection and privacy:

Section 43, *Explanation* (v) “Reasonable security practices and procedures” means, in the absence of a contract between the parties or any special law for this purpose, such security practices and procedures as appropriate to the nature of the information to protect that information from unauthorized access, damage, use, modification, disclosure or impairment, as may be prescribed by the Central Government in consultation with the self-regulatory bodies of the industry, if any.

Section 43, *Explanation* (vi) “Sensitive personal data or information” means such personal information, which is prescribed as “sensitive” by the Central Government in consultation with the self-regulatory bodies of the industry, if any.

It is obligatory to note that not only the aforementioned proposed amendments would pave the way of *self-regulation* in terms of defining what constitute: “reasonable security practices and procedures” and “sensitive personal data or information” but also grant statutory protection to sensitive personal data.

---

<sup>10</sup> These public and private authorities may be referred as ‘data collectors’ or ‘data users’.

<sup>11</sup> Expert Panel submitted its report in August, 2005

Further, the proposed amendments have enlarged the scope of section 66 by making it consistent with the provisions of the Indian Penal Code, 1860, and also providing extent of criminal liabilities in case of data, computer database theft, privacy violation etc. Moreover, newly proposed sub-section (2) of section 72 makes the intermediaries (network service providers) liable for data and privacy violations. Now, such intermediaries to pay damages by way of compensation to the subscriber so affected.

### **1.3.3 The Information Technology Act, 2000 and Privacy Protection: A Critique**

The Information Technology Act, 2000 is not data or privacy protection legislation *per se*. It does not lay down any specific data protection or privacy principles. The Information Technology Act, 2000 is a generic legislation, which articulates on range of themes, like digital signatures, public key infrastructure, e-governance, cyber contraventions, cyber offences and confidentiality and privacy. It suffers from a one Act syndrome.

It would be erroneous to compare the Information Technology Act, 2000 provisions with the European Directive on Data Protection (EC/95/46), OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980, and the Safe Harbor principles of the US.

In fact the Information Technology Act, 2000 deals with the issue of data protection and privacy in a *piecemeal* fashion. There is no an actual legal framework in the form of Data Protection Authority, data quality and proportionality, data transparency etc. which properly addresses and covers data protection issues in accordance with the principles of the EU Directive, OECD Guidelines or Safe Harbor Principles. Accordingly, even if the new proposed amendments to the Information Technology Act, 2000 were adopted, India would still lack a real legal framework for data protection and privacy.