

Position and Perspective of Privacy Laws in India

Bijan Brahmhatt

Student, Final Year, B.Sc. LL.B. (Hons)
Gujarat National Law University
Gandhinagar, Gujarat, India

Gradually the scope of legal rights broadened; and now the right to life has come to mean the right to enjoy life--the right to be let alone.

- Justice Louis Brandeis (1890)

With robust growth and comparatively stable economy, India continues to be a key and fast developing market across the world. Number of foreign companies operating in India grows 100% every year. Yet India is still to embark upon a law that matches to developed nations' legal system and meets investors' expectations. However, the courts in India have used existing laws to afford protection and confer rights to secure a fair privacy to everyone.

The term privacy refers to the use and disclosure of personal information and is only applicable to information specific to individuals. Since personal information is a manifestation of an individual personality, the Indian courts including the Supreme Court of India in *Kharak Singh v. State of U.P.* (AIR 1963 SC 1295), have recognised that the right to privacy as an integral part of the right to life and personal liberty, which is a fundamental right guaranteed to every individual under the Constitution of India. As such, the right to privacy has been given paramount importance by the Indian judiciary and can only be fettered with for compelling reasons such as, security of the state and public interest.

Legal Framework in India

Presently, there is no specific legislation dealing with privacy and data protection. The protection of privacy and data can be derived from various laws pertaining to information technology, intellectual property, crimes and contractual relations.

Privacy under the Constitution of India

In the Indian context, although there is no statutory enactment expressly guaranteeing a general right of privacy to individuals in India, elements of this right, as traditionally contained in the common law and in criminal law is recognized by Indian courts. These include the principles of nuisance,

trespass, harassment, defamation, malicious falsehood and breach of confidence. In addition, several pieces of discrete legislation also recognise this right: for example, the Juvenile Justice Act 2000, which prohibits the publication of names and other particulars of children involved in proceedings under the Act; the Hindu Marriage Act 1955, which imposes similar restrictions on the publication of reports concerning proceedings of matrimonial disputes; and the Copyright Act 1957, which prohibits the unauthorised publication of certain documents, photographs, etc. The Code of Criminal Procedure, 1973, also permits restrictions to be imposed on the publication of reports concerning certain legal proceedings, eg. rape trials.

Under the Indian Constitution, Article 21 of the Indian Constitution is a fairly innocuous provision in itself i.e. "No person shall be deprived of his life or personal liberty except according to procedure established by law" However, the above provision has been deemed to include within its ambit, inter-alia, the Right to Privacy - "The Right to be left alone" (*Rajgopal v. State of TN*, 1994 (6) SCC 632) - as the Supreme Court termed it. The concept of right to privacy finds its genesis in the case of *Gobind v. State of Madhya Pradesh* (AIR 1975 SC 1378), wherein the Supreme Court of India in its ruling, (speaking through Mathew J.) cited the Preamble of the Constitution of India which is designed to "assure the dignity of the individual". Further, in a detailed exposition on Right to Privacy, the Supreme Court in *R. Rajgopal v. State of TN* (1994 (6) SCC 632) laid down that, the right to privacy is implicit in the right to life and liberty guaranteed to a citizen under Art.21 of the Constitution, a citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, childbearing and education among other matters. None can publish (meaning "make known to the public") anything concerning the above matters without his consent, whether truthful or otherwise and whether laudatory or critical, unless they are part of public records. However, the Supreme Court made the above observations in the context of search and surveillance orders, be that as it may, admittedly the Court made its first foray in evolving the concept of Right to Privacy, which in any event would

necessarily have to go through a process of case-by-case development.

Privacy in Tort Law

The Right to Privacy is further encompassed in the field of Torts. The tort of Defamation involves the right of every person to have his reputation preserved inviolate. It protects an individual's estimation in the view of the society and its defenses are 'truth' and 'privilege', which protect the competing right of freedom of speech. Essentially, under the law of torts, defamation involves a balance of competing interests. The only concession for an action, which involves infringement of right to privacy, would be for reasons of, prevention of crime, disorder, or protection of health and morals or protection of rights and freedom of others.

Privacy in Contract Law

There exist certain other means by which parties may agree to regulate the collating and use of personal information gathered, viz. by means of a "privacy clause" or through a "confidentiality clause" Accordingly, parties to a contract may agree to the use or disclosure of an individual's personal information, with the due permission and consent of the individual, in an agreed manner and/or for agreed purposes. Under Indian laws, the governing legislation for contractual terms and agreements is the Indian Contract Act. Therefore, in a contract which includes a "confidentiality clause" i.e. where an organization/company agrees to maintain the confidentiality of information relating to an individual, any unauthorized disclosure of information, against the express terms of the agreement would amount to a breach of contract inviting an action for damages as a consequence of any default in observance of the terms of the contract.

In the case of an insurance contract, globally, contracts of Insurance are contracts of "Utmost good faith" (*Uberrimae Fidei*) and the contract is voidable where all material facts are not disclosed. However, the duty of utmost good faith is reciprocal and the insurance company has a corresponding duty to disclose clearly the terms of its offer and duly abide by them. Therefore an insurance proposal, which contains a confidentiality clause regarding personal information provided by the customer, cannot be disclosed without his prior consent. Any breach of such term would invite an action for breach of contractual terms by the insurer-customer. In India, a state-owned insurance corporation would typically include in its proposal; an Indemnity clause whereby the customer agrees "that such authority (corporation) having such knowledge or information (regarding the customer), shall at any time be at liberty to divulge any such knowledge or information to the corporation". By agreeing to the above clause, the insurance corporation indemnifies itself against any disclosure related ac-

tion by the customer, however, such clause/term for disclosure should be construed narrowly and any mala fide disclosure could invite an action against the company, which discloses the information, based on equity and good faith, despite the presence of a standard indemnity clause in the original agreement.

In regard to a customer- insurance company relationship, an insurance company may, solicit personal information about an individual wherein details could be sought, relating to an individual's family, cultural background, ethnic origin, caste, childhood, education, medical history, information regarding one's immediate family, their age, profession etc. or, in case of data processing companies, there may be queries with regard to an individuals' professional pursuits, income, investment decisions, preferences, spending patterns and so on. Despite an express authorization from their customers, with regard to sharing of personal information by corporate entities, there may still be instances where disclosure of certain sensitive and embarrassing information could invite legal action from an individual, claiming that the actions of a company which made an unauthorized disclosure resulted in causing such mental agony, anguish, and social stigma, which he would not have otherwise had to bear or face.

Privacy Obligations under Specific Relationships

There are instances of specific inter-personal relationships wherein one party might be obligated to maintain a certain measure of confidentiality. A doctor-patient, husband-wife, customer-insurance company or an attorney-client relationship; are instances where there exists a strong ethical obligation on the part of one party to protect the privacy of information relating to an individual which may expose him to social humiliation and/or ridicule. In the case of an attorney-client relationship, professional ethics prescribe that certain communications and conversations between the attorney and his client must remain outside the ambit of public knowledge and should be maintained as such. The above principle also receives legal recognition in S.126 of the Indian Evidence Act 1871.

In the case of *X v. Hospital Z* (1998 (8) SCC 296), the Supreme Court held, "Right of Privacy may, apart from contract, also arise out of a particular specific relationship which may be commercial, matrimonial or even political. The Court further went on to hold that "... disclosure of even true private facts has the tendency to disturb a person's tranquility. It may generate many complexes in him and may even lead to psychological problems. In the face of these potentialities, and as already held by this Court in its various decisions, the right to privacy is an essential component of the right to life as envisaged by Article 21.

From the above discussion, there emerge two critical elements with regard to the assessment of the fairness of disclosure of personal information:

- i. The nature and sensitivity of information with regard to an individual and the reasonable consequence of such disclosure
- ii. The purpose or rationale for disclosing personal information by the organization/company making such disclosure

Relevant Provisions under various Statutes

a. Information Technology Act, 2000: The Information Technology Act (hereafter IT Act) is often presented, in India, as the text regulating data protection under Indian Law. This Act has been enacted in the Fifty first Year of the Republic of India. It received the assent of the President on the 9th June, 2000 and is effective as of 17th October, 2000. This Act is based on the Resolution A /RES/51/162 adopted by the General Assembly of the United Nations on 30th 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 aim of the IT Act was to set up India's first ever information technology legislation.

The IT Act provides for safeguard against certain of breaches in relation to data from computer systems. The said Act contains provisions to prevent the unauthorized use of computers, computer systems and data stored therein. The section creates personal liability for illegal or unauthorized use of computers, computer systems and data stored therein. However, the said section is silent on the liability of internet service providers or network service providers, as well as entities handling data. As a result, the entities responsible for safe distribution and processing of data like the vendors and outsourcing service providers are out of the purview of this section. The liability of the entities is further diluted in Section 79 by providing the criteria of "knowledge" and "best efforts" before determining the quantum of penalties. This means that the network service provider or an outsourcing service provider would not be 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. It may be noted that if there is any alleged violation of the IT Act by a company, its key employees (managers and directors) are made personally liable for intentional or negligent act resulting in the violation of the IT Act.

With regard to damages available in the event of a breach of data privacy under the said Act, the maximum penalty for illegal and unauthorized use of computer data is approximately \$222,000/-. The law makes no differentiation

based on the 'intentionality' of the unauthorized breach, and no criminal penalties are associated with the breach. Section 65 offers protection against intentional or knowing destruction, alteration, or concealment of computer source code while Section 66 makes alteration or deletion or destruction of any information residing in a computer an offence. Both sections 65 and 66 are punishable with criminal penalties including imprisonment up to 3 years or a monetary penalty of up to \$440,000/-.

b. Indian Penal Code: The Indian Criminal law does not specifically address breaches of data privacy. Under the Indian Penal Code, liability for such breaches must be inferred from related crimes. For instance, Section 403 of the India Penal Code imposes criminal penalty for dishonest misappropriation or conversion of "movable property" for one's own use.

c. Intellectual Property Laws: The Indian Copyright Act prescribes mandatory punishment for piracy of copyrighted matter commensurate with the gravity of the offence. 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. Fines in the minimum amount of approximately \$1,250, up to a maximum of approximately \$5,000 may be levied 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.

It is pertinent to mention here that the Indian courts recognise copyright in databases. It has been held that compilation of list of clients/customers developed by a person by devoting time, money, labour and skill amounts to "literary work" wherein the author has a copyright under the Copyright Act. As such if any infringement occurs with respect to data bases, the outsourcing parent entity may have recourse under the Copyright Act also.

d. Credit Information Companies Regulation Act, 2005("CICRA") As per the CICRA, the credit information pertaining to individuals in India have to be collected as per privacy norms enunciated in the CICRA regulation. Entities collecting the data and maintaining the same have been made liable for any possible leak or alteration of this data. Based on Fair Credit Reporting Act and Graham Leach Bliely Act, the CICRA has created a strict framework for information pertaining to credit and finances of the individuals and companies in India. The Regulations under CICRA which provide for strict data privacy principles have recently been notified by the Reserve Bank of India.

Industry Initiative

In India, the efforts at complying with the demands of adhering to privacy laws have originated mainly from the private sector rather than the Government. In the absence of a

specific legislation, the Indian software and outsourcing industry has been taking initiatives on its own that would provide comfort to the foreign clients and vendors.

The National Association of Service & Software Companies (NASSCOM) is India's national information technology trade group and has been the driving force behind many private sector efforts to improve data security. For example, NASSCOM has created a National Skills Registry which is a centralized database of employees of the IT services and BPO companies. This database is for verification (with independent background checks) of the human resources within the industry. Further, a self regulatory organisation has been launched which will establish, monitor and enforce privacy and data protection standards for India's business process outsourcing industry. The organisation has already completed its initial round of funding and the final rollout phase including industry membership is underway.

In the Indian context, the rapidly growing services sector has resulted in both Indian and trans-national corporate entities building up vast, exhaustive and detailed customer databases with a view to providing personalized services such as insurance, personal banking, credit cards etc. These databases contain confidential personal information and may be used by corporates for their own purposes or for that of its affiliates. Also, these databases form a valuable corporate asset, which finds many takers in the market for individual information.

In this regard, any use, disclosure and retention of such information needs to be strictly regulated, through an established privacy enforcement regime. Any prospective Indian privacy law would need to incorporate several facets of the above model, which, comprehensively deals with the collection, and use of personal information. With the emergence of an increasingly uniform set of norms governing commercial legal issues across the globe, it becomes imperative for Indian law makers and the legislature to take note of the void that prevails in the critical area of individual privacy protection.

Attempts to bring in change

In the Fall of 2003 discussions among the Indian government, industry associations, and legal experts resulted in a "go slow" approach. Instead of proceeding directly to a new comprehensive, EU-type statute, it was decided to institute an interim regime that would either consist of a revision of the Information Technology Act 2000, or would emulate the Safe Harbor Principles agreed between the EU and the United States. "While framing the legal mechanism, India could consider the minimalist approach. The idea is to ensure that India does not come across as a country bogged

down by too many regulations. The emphasis has to be on projecting a flexible regime that enables the development of the IT sector. As a result of these discussions, the industry offered an "action plan" which would commence with Nasscom identifying Indian companies operating in the EU, and consolidating the data protection provisions in their contracts for dissemination to the Indian out-sourcing industry. A group of legal experts would review the present legal framework and suggest modifications. And the government would analyze the Safe Harbor arrangement in place between the EU and the United States, so as to understand its comprehensiveness and the steps necessary for a dialog with the EU on execution of a similar agreement with India.

Need for Specific Privacy Law

There exists in India an impending need to frame a model statute which safeguards the Right to Privacy of an individual, especially given the emergence of customer-service corporate entities which gather extensive personal information relating to it's customers. It's evident that despite the presence of adequate non-mandatory, ethical arguments and precedents established by the Supreme court of India; in the absence of an explicit privacy statute, the right to privacy remains a de facto right, enforced through a circuitous mode of reasoning and derived from an expansive interpretation of either Constitutional law or tort law.

The urgency for such a statute is augmented by the absence of any existing regulation which monitors the handling of customer information databases, or safeguards the Right to Privacy of individuals who have disclosed personal information under specific customer contracts viz. contracts of insurance, credit card companies or the like. The need for a globally compatible Indian privacy law cannot be understated, given that trans-national businesses in the services sector, who find it strategically advantageous to position their establishments in India and across Asia. For instance, India is set to emerge as a global hub for the setting up and operation of call centers, which serve clients across the world. Extensive databases have already been collated by such corporates, and the consequences of their unregulated operations could lead to a no-win situation for customers in India who are not protected by any privacy statute, which sufficiently guards their interests. Even within the present liberal global regulatory paradigm, most governments would be uncomfortable with a legal regime, which furthers commercial interests at the cost of domestic concerns.

Conclusion

In the privacy and data protection area, the winds of change are blowing across India, and they are likely soon to alter the landscape. But the new shape of that landscape is not yet clear. The near future is likely to see major modifica-

tions to the Information Technology Act 2000 and/or a proposal to the EU for a Safe Harbor–India regime. The long-term shape of Indian data protection law may depend on the success (or lack of it) that the short-term solution enjoys. But, one way or another, Indian privacy law is likely to change dramatically in the next few years.

References

Jean-Jacques and Debroy, B. eds. 2000. *Some issues in law reform in India*, Governance, Decentralization and Reform in China, India and Russia, Dethier : Kluwer Academic Publishers.

Warren, S and Brandeis, L.eds. 2000 *The Right To Privacy*, 4 Harvard Law Review 193 (1890)

Kumaraguru, I and Cranor, I. *Privacy Perceptions in India and the United State: An Interview Study*, p. 9, available at http://www.cs.cmu.edu/~ponguru/tprc_2005_pk_lc_en.pdf

Privacy & Human Rights, An international survey of privacy laws and developments, Electronic Privacy Information Center, 2004,