CHAPTER - X

CONCLUSIONS AND SUGGESTIONS

10.0 Conclusions

Privacy is the ability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves selectively. The boundaries and content of what is considered private differ among cultures and individuals, but share basic common themes. Privacy is sometimes related to anonymity, the wish to remain unnoticed or unidentified in the public realm. When something is private to a person, it usually means there is something within them that is considered inherently special or personally sensitive. The degree to which private information is exposed therefore depends on how the public will receive this information, which differs between places and over time. Privacy partially intersects security, including for instance the concepts of appropriate use, as well as protection, of information.

The right not to be subjected to unsanctioned invasion of privacy by the government, corporations or individuals is part of many countries' privacy laws, and in some cases, constitutions. Almost all countries have laws which in some way limit privacy; an example of this would be law concerning taxation, which normally requires the sharing of information about personal income or earnings. In some countries individual privacy may conflict with freedom of speech laws and some laws may require public disclosure of information which would be considered private in other countries and cultures. Privacy may be voluntarily sacrificed, normally in exchange for perceived benefits and very often with specific dangers and losses, although this is a very strategic view of human relationships. Academics who are economists, evolutionary theorists, and research psychologists describe revealing privacy as a 'voluntary sacrifice', for instance by willing participants in sweepstakes or competitions. In the business world, a person may volunteer personal details (often for advertising purposes) in order to gamble on winning a prize. Personal information which is voluntarily shared but subsequently stolen or misused can lead to identity theft.
Privacy, as the term is generally understood in the West, is not a universal concept and remained virtually unknown in some cultures until recent times. Most cultures, however, recognize the ability of individuals to withhold certain parts of their personal information from wider society - a fig leaf over the genitals being an ancient example.

The right of privacy has been gaining recognition, though lately, and it has been declared as a part of Art. 21, though the Indian Constitution does not speak in explicit terms. Art. 21 which says “No person shall be deprived of his life and personal liberty according to procedure established by law”. The right to privacy can be exercised only if the violator is the state and not a private individual or institution. This right being not absolute can be interfered in the interest of health and medical standards. This right does not prohibit any publication of matter which is of general interest.

So far the law relating to the right to privacy has been relegated to a penumbral status and is still going through the state of infancy. It is high time that the government and information technology industry come together to check out ways and means to curb the problem of intrusion of privacy. Our legislatures have to protect privacy rather than laws that facilitate violation of individual’s privacy in the name of governmental functions.

Privacy is a fundamental human right recognized in the UN Declaration of Human Rights, the International Covenant on Civil and Political Rights and in many other international and regional treaties. Privacy underpins human dignity and other key values such as freedom of association and freedom of speech. It has become one of the most important human rights issues of the modern age. The growing importance, diversity and complexity of this fundamental right are reflected. However, the right to privacy is under serious threat due to the emergence of information technology. The application of various electronic gadgets has made the surveillance of the activities of the individuals very easy. The existing laws have been found to be ineffective in dealing with this problem and this has necessitated enactment of new laws.

Nearly every country in the world recognizes a right of privacy explicitly in its Constitution. At a minimum, these provisions include rights of inviolability of the home.
and secrecy of communications. Most recently-written Constitutions such as South Africa's and Hungary's include specific rights to access and control one's personal information. In many of the countries where privacy is not explicitly recognized in the Constitution, such as the United States, Ireland and India, the courts have found that right in other provisions. In many countries, international agreements that recognize privacy rights such as the International Covenant on Civil and Political Rights or the European Convention on Human Rights have been adopted into law.

In the early 1970s, countries began adopting broad laws intended to protect individual privacy. Throughout the world, there is a general movement towards the adoption of comprehensive privacy laws that set a framework for protection. Most of these laws are based on the models introduced by the Organization for Economic Cooperation and Development and the Council of Europe.

In 1995, conscious both of the shortcomings of law, and the many differences in the level of protection in each of its States, the European Union passed a Europe-wide directive which will provide citizens with a wider range of protections over abuses of their data. The directive on the "Protection of Individuals with regard to the processing of personal data and on the free movement of such data" sets a benchmark for national law. Each EU State had to pass complementary legislation by October 1998.

The Directive also imposes an obligation on member States to ensure that the personal information relating to European citizens is covered by law when it is exported to and processed in countries outside Europe. This requirement has resulted in growing pressure outside Europe for the passage of privacy laws. More than forty countries now have data protection or information privacy laws. More are in the process of being enacted.

The evidence gathered during this study showed clearly that the success or failure of privacy and data protection is not governed by the text of legislation, but rather by the actions of those called upon to enforce the law. It cannot be stressed enough that supervisory authorities must be given an appropriate level of responsibility for this arrangement to work. The stronger, results oriented approach aims to protect data...
subjects against personal harm resulting from the unlawful processing of any data, rather than making personal data the building block of data protection regulations. It would move away from a regulatory framework that measures the adequacy of data processing by measuring compliance with certain formalities, towards a framework that instead requires certain fundamental principles to be respected, and has the ability, legal authority and conviction to impose harsh sanctions when these principles are violated.

Data protection is an issue that is gaining increasing importance as our transnational exchange of private information grows. While the E. U. has adopted stringent legislation to protect data, and the U.S. has reached agreement with the E.U. to offer protection, the Indian laws remain unsatisfactory. It is anticipated that India will soon enact legislation which will provide acceptable protection to private data. The issue that remains to be dealt with in the Indian context is, unfortunately, far larger than the enactment of strong protectionist laws. Laws act as a deterrent to wrongful conduct if they are applied with certainty and speed: both sadly deficient in the Indian judicial system. Unless addressed, the systemic problems of enforcement in India, and specifically, of unresolved cases due to court delays, will continue to render India's data protection laws inadequate. Cyber Infringement Courts, specialized courts with jurisdiction over a intellectual property and data protection issues, are a necessary solution to India's enforcement problems. India must expediently adopt this system of specialized courts in order to render adequate protection to data and maintain its growing presence in the global technology arena.

Cloud computing has significant implications for the privacy of personal information as well as for the confidentiality of business and governmental information. A principal goal of this analysis is to identify privacy and confidentiality issues that may be of interest or concern to cloud computing participants. While the storage of user data on remote servers is not new, current emphasis on and expansion of cloud computing warrants a more careful look at its actual and potential privacy and confidentiality consequences.

Many experts argue that cloud computing is more secure than the various traditional methods of data storage such as servers, hard disks, etc., though organisations
still take the risk of data being stolen by any outsider hacking into the security system of the cloud. The main reason why organisations are not opting for cloud services is the lack of security. However, the traditional storage methods also present risks—the servers can also be hacked into by an outsider and hard disks can also crash and destroy the data stored.

In the Indian scenario, as cloud computing is a novel concept there is no law which specifically governs it and the law at present lacks clarity. Questions as to the applicable law and the jurisdiction of the court still remain unanswered. Still, organisations are switching from traditional methods of storage to cloud computing because of the cost efficiency. The proposition deduced here is that cloud computing may not be ideal for all organisations because of the various issues raised but, it is economical and convenient for global organisations to use in order to store data which can be accessed from any part of the world at any time.

After reviewing some of the "cyberspace" legislation, it is not surprising to find that the legislation in this field lacks clarity. The Digital Millennium Copyright Act of the United States has clearly defined the standard of knowledge an ISP is required to possess for it to be held liable for illegal third party activities. The Digital Millennium Copyright Act allows ISPs to terminate the accounts of individuals who infringe copyrights on a regular basis. Furthermore, in the United States, ISPs have to register an agent with the appropriate office so they can receive information of copyright infringements. This eliminates the possibility of an ISP being caught unaware of third party infringements.

As is seen, the EU Directive has some loopholes that need to be closed. The most troublesome of which include, a lack of a "notice and takedown" procedure, which threatens freedom of expression; and the fact that the current regime may actually promote unfair competition in some situations. The lack of a notice and take down procedure causes the ISPs to become a sort of censorship body, in order to avoid liability when they opt to take down a Web page upon receipt of a claim regarding the content on that page. This threatens freedom of expression as long as customers are without protection against unfounded complaints. Unfair competition may be promoted in cases
where companies engage in a form of commercial war in cyberspace, lobbing bad faith claims against their competitor's Web content.

The Credit Information Companies (Regulation) Act 2005, although it is not yet fully operational, includes privacy principles which cover most usual data protection rights, though only in relation to the context of credit reporting. There is otherwise as yet no significant legislation protecting personal information in India, though some provisions in the ITAA2008 may emerge as significant depending on regulations made and implementation, particularly concerning data security. There is no special protection for personal information imported into India from other jurisdictions.

There is an effective right of access to personal information in the public sector, under the Right to Information Act 2005, and this right of access is probably the most significant aspect of data protection in India at present. There is also protection within India against telemarketing through the Telecom Unsolicited Commercial Communications Regulations 2007. Significant though these areas are, it cannot be said that privacy principles apply to most aspects of Indian life.

The Central Information Commission, State Information Commissions, and the network of Information Officers in all public authorities in India, constitute an effective means of administering and enforcing the access principle. The CIC actively enforces the law by the use of both compensation and penalties. If the Right to Information Act 2005 had added to it the rest of the set of data protection principles, India would be likely to have an effective enforcement system for data protection. Neither the National Human Rights Commission nor the Cyber Regulation Appellate Tribunal seems to be as promising as the basis for a data protection authority. The Do-Not-Call register seems to be developing effective enforcement, but that is in a much specialised area.

The Credit Information Companies (Regulation) Act 2005, although it does include a full set of privacy principles, is lacking in comprehensive enforcement measures. It relies almost entirely on prosecution of offences, either through the courts or administratively by the Reserve Bank. There is no obvious way for complaints to be made. The Reserve Bank has extensive directive powers, but is not a consumer protection
agency and its interests are more obviously in creating a modern credit economy than in protecting consumer privacy. However, the system is untested, and it is necessary to wait and see.

There is as yet no significant self-regulation for the purposes of privacy protection in India. There are no aspects of India's data protection which would unequivocally be regarded as 'adequate' by European Union standards as yet, though further investigation might indicate that there are some sectoral areas of adequacy. This could also change as rules are made under existing legislation. The most likely candidates (in decreasing order of likelihood) might be: The credit reporting system, but only after it has been tested in practice; The right of access (but only in relation to public authorities); The implementation of the security principle via both compensatory provisions (subject to how Section 43A is implemented) and offences; The provisions concerning opting out from direct marketing.

India is still at a very early stage of developing personal data protection, though some of the signs are promising. Balanced against this must be the increases in surveillance powers.

10.1 Suggestions

From the above discussion the following suggestions have been made

1) Need for a Constitutional Amendment: There is need for a constitutional amendment whereby right to privacy can be guaranteed expressly by insertion of a new provision. Such an amendment is necessary so as to give recognition to the right to privacy. Only then personal liberty as guaranteed by Art. 21 can be more meaningful.

2) Evolving National Policy: India needs a comprehensive policy guaranteeing individuals the right to control the collection and distribution of their personal information. Legislation which incorporates the basic tenets of fair information practices is a vital component of this policy. These tenets give individuals the right to limit data collection, data transfers, and secondary uses of the data; the
right to access one's personal data and to make corrections; the right to have one's personal data maintained securely; and the right to be informed of data collection and transfer. The legislation would therefore place restrictions on the collection and use of personal data by the users of personal information. Personal information users would be required to explicitly inform individuals when personal information is being collected and how this information might be used. Legislation would require that personal information users give individuals an opportunity to prevent further dissemination of their personal information. Accordingly, there would be appropriate restrictions on the online publication and collection of personal information. Informational privacy interests and autonomy interests and data protection interests need to be safeguarded with appropriate legal mechanisms to ensure security of data and exchange of confidential or personal sensitive information in the cyberspace.

3) Freedom of speech and expression over internet ought to be maintained and development of sophisticated technological and legal solutions shall pave way for securing online privacy and data. Reasonable restrictions should remain reasonable on the anvil of law and should not fetter growth of internet and communications. Internet censorship should only be invoked in the cases of dire necessity on justifiable grounds such as preserving national sovereignty, public order and safety.

4) There is a need of a comprehensive law which would provide an enforcement mechanism, which would establish sanctions against violators and offer redress for aggrieved individuals. Most effective would be legislation providing a private right of action for aggrieved individuals along with the administrative enforcement powers of a government regulatory authority.

5) Although such a comprehensive privacy policy is necessary to guarantee the individual's right to control the collection and distribution of personal information, there is a need for the individuals concerned to exercise this control. Online users will still need to take responsibility for their electronic
communications. They will need to be cautious about the content of these communications, and use appropriate security measures, such as encryption, to safeguard their security. Individuals will also need to decide how much personal information to reveal when registering at Internet sites and participating in commercial transactions. By anticipating the hazards of online use and utilizing the legal protections previously outlined, individuals will be able to take full advantage of the many educational, social, and commercial opportunities available now, and in the future, throughout cyberspace.

6) Online communications are not private unless one uses encryption software. But most encryption programmes are not user friendly and can be inconvenient to use. No regulatory mechanism of the state would be adequate to protect the right to privacy of the individuals. Hence, the individuals are required to take certain precautions: Thus,

a) They should not provide sensitive personal information (phone number, password, address, credit card number, social security number, health information, date of birth, vacation dates, etc.) in chat rooms, forum postings, e-mail messages, or in your online biography.

b) While ‘surfing the internet’, sending electronic mail messages and participating in online forums, it’s easy to be lulled into thinking that these activities are private. However, any step along the way, online messages could be intercepted and activities monitored in the vast untamed world of cyberspace.

c) If anyone thinks that the ‘delete’ command makes the e-mail messages disappear, it is a wrong notion. Such messages can still be retrieved from back-up systems. Software utility programmes can retrieve deleted messages from the user’s hard drive. If one is interested about permanently deleting messages and other files on the programme, he should use a file erasing programmes.
d) Children who are online users must be taught by parents about appropriate online privacy behaviour. Caution them against revealing information about themselves and their family.

e) User must be made aware of voluntarily sharing information and no data should be downloaded without express consent. Always access secure websites at the time of transmitting sensitive personal information such as credit card number over the internet. Always take advantage of privacy protection tools.

7) Data protection and privacy rights are two of the most important rights conferred by any civilized nation. Every individual and organisation has a right to protect and preserve her/its personal, sensitive and commercial data and information. This is more so regarding health information and details that is required to be kept secret by laws like Health Insurance Portability and Accountability Act of 1996 (HIPAA) in United States. India does not have a dedicated law like HIPPA and presently HIPPA compliances in India are not followed. Similarly, we have no dedicated medical privacy law in India that can safeguard the sensitive health related information of the patients. In short, we have no dedicated data protection laws in India, data privacy laws in India and privacy rights and laws in India.

8) As a recommendation, it is proposed that a notice and take down procedure modelled after the DMCA be established, including notice to specialized bodies within the Member States' administrative structures or professional organizations. Regarding the second Achilles heel of the EU Directive, in order to have a complete protection for all the parties involved, a "put back procedure" should be initiated. Such a procedure should give the owners of disabled Web sites the chance to exercise a defence and at least stave off an unwarranted blocking or removal of their content. Finally, liability must be imposed upon persons who intentionally transmit false or unfounded notices which lead to the removal of a Web page content.
9) The Indian position in the "cyberspace" legislation must be made more explicit. It must clearly require an ISP to have actual knowledge of any infringing act to be held liable. To make it convenient for ISPs, they could be asked to designate an agent with the requisite authority to receive complaints regarding offenses committed on the Internet. This will ensure that the ISP has sufficient knowledge of the abuses on the Internet. The Australian Act gives due importance to the financial gain made by ISPs along with the nature of the relationship between an ISP and a third party infringer. Similarly, the Indian Act must include sections that address the financial aspect of the transaction, and the relationship between an ISP and a third party, because this is vital to determining the identity of the violator. The American concept of contributory infringement can also be incorporated into the Indian Act so that if any person "with knowledge of the infringing activity, induces, causes, or materially contributes to the infringing conduct of another," the person can be made liable. And as in the Australian Act, an ISP must not be held liable unless it determines the content of the material.

10) In order to be exempt from liability, the Indian Act requires the service provider to exercise "due diligence" to prevent the commission of copyright infringement. The Act does not provide the meaning of the term "due diligence." If "due diligence" means policing each and every aspect of the Internet, it can lead to loss of privacy and can ultimately have a disastrous effect. There is a need for a consensus on the meaning of the term due diligence because the primary function of ISPs is to build the Internet, not to play the role of a policeman. Consequently, "due diligence" should be interpreted narrowly. If the behaviour of an ISP is reasonable, then that ISP should not be held liable for each and every activity on the Internet. The laws should be pragmatic because an ISP cannot be expected to monitor all the activities on the Internet.

11) However, despite the importance of these fields, till now we lack legal frameworks in the fields of data security, data protection and privacy protection. We urgently need to formulate data protection law in India and privacy laws in India. At the policy level as well privacy rights and data protection rights have
been ignored in India. In fact, an Indian national privacy policy is missing till now. Even legislative efforts in this regard are not adequate in India. A national privacy policy of India is urgently required.

12) The ball is again in the court of judiciary and it has to play a proactive role once again. The Supreme Court of India must expand privacy rights in India as that is the need of hour. Fortunately, the issue is already pending before it and there would not be much trouble in formulating a privacy framework for India. However, in the ultimate analysis, it is the constitutional duty of Indian Parliament to do the needful in this direction. Indian Parliament must enact sound and effective privacy and data protection laws for India as soon as possible.

If the above suggestions are implemented through appropriate measures, it is sincerely hoped that the right to privacy can be protected more effectively.