ISSN: 0976-3570

Protection of Privacy in the Electronic Age: A Legalistic View

Dr. Vijaya Chandra Tenneti[1]

I. Introduction:

The development in information technology and methods of communications has a direct bearing on the concept of right to privacy. With the unprecedented information revolution and advances in computers and telecommunications there has been a dramatic increase for information that can be stored, collated, accessed and retrieved almost instantaneously. Not only public, but also private bodies are holding an enormous amount of personal information. Right to safeguard one's privacy has become all the more relevant with the onset of the internet and e-commerce. The Internet, with all the benefits of anonymity, reliability and convenience has become a potential ground for illegal gainful purposes, either monetary or otherwise.

The unbridled and uncontrolled expansion of technological tools of this electronic age, has enabled everything and every information and data of individuals to open up with accessibility to tap and watch. The cyber technology has brought in its fold certain inherent dangers to privacy. The new technologies have enhanced the possibilities of invasion into the privacy of individuals and provided new tools in the hands of unscrupulous users. Individual privacy, particularly, in the cyber space, is at a greater stake than ever before. Computer and internet can be used to amass huge amount of data regarding people and profile it in various ways, commodify it and deal with it in a manner which could violate individual's privacy. The concept of right to privacy and the need for its protection is a product of increasingly individualistic society where the personal, intellectual and spiritual facets of the human personality have gained recognition and the law has to expand to give protection to these needs. The rise in the case of privacy infringement can also be attributed to the decline in professional ethics and moral standards, like in any other fields of human activities.

The surveillance potential of powerful computer systems promoted demands for specific rules governing the collection and handling of personal information, to protect the privacy of individuals. It is sordid to note that, the law is lagging behind in this direction.

II. Privacy— A Conceptual Frame Work:

Earlier, law afforded protection only against physical interference with a

---

1 Assoiate Professor of Law, University College of Law, Kakatiya University, Warrangal.

person or his property. But with radical changes in the means of communication and communication networks, the need for privacy and its recognition as a 'right' has come to the forefront[2]. As early as 1890, Justice Louis Brandeis of the US Supreme Court articulated the concept of privacy, urging that it was the individual's right to be let alone'. Privacy is the most comprehensive of the rights of man and it is the right most valued by civilized man[3].

Privacy is a fundamental human right. It is recognized around the world in diverse regions and cultures. Though the whole world is yet to arrive at an agreed definition of privacy, the advocates of 'right to privacy' have agreed that the meaning of privacy is dependent on a nation's culture. Thus, the definition of privacy has been varying depending upon a nation's cultural setting.

Privacy is one of the most difficult issues to be defined precisely. Depending upon the context and environment, definitions of privacy vary widely. Protection of Privacy is frequently seen as a way of drawing the line at how far society can intrude into a person's affairs. It involves, to be sure, some idea of control of information about one-self- that certain information is private and is not to be publicized to one's embarrassment, humiliation or injury. Privacy has also something to do with prevention of certain kinds of intrusion into the individual's life. Privacy, may also involve the concept of autonomy- the individual's right to make certain decisions free from any regulations[4]. Alan F. Westin[5] defined privacy as, "the desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitude and their behaviour to others.

The term 'privacy' has been described as 'the rightful claim of the individual to determine the extent to which he wishes to share of himself with others. It means his right to withdraw or to participate as he sees fit. Adam Carlyle Breckenridge considers it, the individual's right to control dissemination of information about himself[6]. Yet another definition of privacy is, "Zero relationship between two or more persons in the sense that there is no interaction on communication between them if they so choose[7]. The concept of privacy is used

2 Raman Mittal and Neelatpal Deka, "Cyber Privacy", in S.K. Verma and Raman Mittal (ed), Legal Dimensions of Cyber Space, (2004), p.199.

3 Olmstead v. United States (1928),

4 William Cohen, David. J. Constitutional Law: Civil Liberty and Individual Rights, 5th Ed., New York Foundation Press, 2002.

5 (http://www.privacyinternational.org/survey/phr 98

6 Adam Carlyle Breckenridge, The Right to Privacy, 1971, quoted in Madhavi Divan, "The right to Privacy in the Age of Information and Communications", 12, 4 SCC(j), (2002)

7 Edward Shils, "Privacy: Its Constitution and Vicissitudes", 31, 2 Law and Contemporary Problems, Spring 1966

to describe not only rights purely in the private domain between individuals but also constitutional rights against the State.

The Calcutt Committee in the UK adopted its definition on privacy as, "the right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication of information"[8].

Keeping in view all modern developments in Information and communication revolution, privacy in cyberspace can be described as the desire of every individual for virtual space where one can be free of interruption and intrusion and where one can control the time and manner of disclosures of personal information.

III. Protection of Privacy— The International Legal Regime:

The concept of privacy as a human right has been recognized by various international instruments concerning human rights. The 1948 Universal Declaration of Human Rights, which specifically protects territorial and communications privacy, proclaims in Article 12 of the Declaration that: "No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attack on his honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks".

In similar vein, Article 17 of the International Covenant on Civil and Political Rights, Article 14 of the UN Convention on Migrant Workers, Article 16 of the UN Convention on Protection of the Child- all have equally and emphatically declared in unequivocal terms, the individual's right to privacy.

Apart from these, there are several regional international legal instruments on human rights, which seek to protect the right to privacy. Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, 1950 provides:' Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except as in accordance with the law and is necessary in a democratic society in interest of national security, public safety or the economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'.

Similarly, Article 11 of the American Convention on Human Rights also sets out the right to privacy in terms, similar to the Universal Declaration of Human Rights.

---

8 Report of the Committee on Privacy and Related Matters, Chiarman David Calcutt QC, Cmnd. 1102, at 7.

As a sequel to the recent developments, particularly, in the field of information and communication technology, the UNs General Assembly adopted a set of draft 'guidelines for the regulation of computerized personal data profiles'. Divided into two sections, the first section of these guidelines covers 'principles concerning the minimum guarantees that should be provided in national legislations'. These 'principles' echo those put forward by both the Council of Europe Convention and the Organization for Economic Cooperation and Development (OECD) Guidelines. Further, the UN General Assembly guidelines added three more principles to the existing guidelines:

1. 'Principle of non-discrimination' – sensitive data, such as racial or ethnic origin, should not be compiled at all.
2. 'Power to make exceptions'– justified only for reasons of national security, public order, public health or morality.
3. 'Supervision and sanctions'– the data authority 'shall offer guarantees of impartiality, independence vis-à-vis persons or agencies responsible of processing.

IV. The Organization of Economic Cooperation and Development (OECD) Guidelines on Privacy:

The Organization for Economic Cooperation and Development, which has one of the primary objective of developing guidelines on basic rules governing the trans- border flow and the protection of personal data and privacy. These guidelines were drafted in 1979 and adopted in 1980. The OECD guidelines consist of eight basic principles which are as follows:

1. Collection Limitation Principle: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and where appropriate, with the knowledge or consent of the data subject.
2. Data Quality Principle: Personal data should be relevant to the purpose for which they are to be used and to the extent necessary for those purposes, should be accurate, compete and kept up-to-date.
3. Purpose Specification Principle: The purpose for which personal data are collected should be specified not late than at the time of collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasions of change of purpose.
4. Use Limitation Principle: Personal data should not be disclosed, mad available or otherwise used for purposes other than those specified in accordance with principle 3, except: a) with the consent of the data subject or b) by the authority of law.

5. Security Safeguards Principle: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

6. Openness Principle: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7. Individual Participation Principle: An individual should have the right a). To obtain from a data controller, or otherwise confirmation of whether or not the data controller has data relating to him b). To hover communicated to him, data relating to him i). within a reasonable time ii). at a charge, if any, that is not excessive iii). in a reasonable manner and iv). in a form that is readily intelligible to him c). to be given reasons if a request made under sub-paragraphs a and b is denied, and to be able to challenge such denial and d). to challenge data relating to him and, if the challenge is successful, to have the data erase, rectified, completed or amended.

8. Accountability Principle: A data controller should be accountable for complying with measures which give effect to the principles stated above.

V. Right to Privacy and Indian Constitution:

The Constitution of India does not guarantee the right to privacy as specific fundamental right. However, the Supreme Court has carved out a constitutional right to privacy by a creative interpretation of right to life envisaged under Article 21of the Constitution. The concept of privacy as a fundamental right first evolved in the sixties. Kharak Singh Vs. State of Utter Pradesh[9], is one of such cases, wherein, it has been held by the Supreme Court that, the term 'liberty; spelled out in Article 21 was comprehensive enough to include privacy.

Elucidating the nature and dimensions of individual privacy, Justice Mathew in Govind Vs. State of Madhya Pradesh, observed[10] 'any right to privacy must encompass and protect the personal intimacies of the home, the family, marriage, motherhood, procreation and child bearing. This list was however, not exhaustive.

The decision of the apex court in Rajagopal Vs. State of Tamil Nadu[11], is a watershed in the development of privacy law in India, where for the first time the court has discussed about the right to privacy in the context of freedom of

9 (1964) 1 SCR 332.
10 AIR 1975, SC 1378
11 AIR 1995 SC 264

press. The court held that every citizen had a right to safeguard the privacy of his own. The right to privacy has since been widely accepted as implied in our Constitution[12].

Analyzing the development of privacy laws in India, one can note that these laws evolved basically from two sources: the common law of torts and the constitutional law. In common law, a private action for damages for unlawful intrusion of privacy is maintainable. Under the constitutional law, the right to privacy is implied in the fundamental right to life and liberty.

VI. Right to Privacy and Information Technology Act, 2000:

Though the Information Technology Act, 2000 has been basically enacted to regulate the E-Commerce, it incidentally focuses little attention on certain ancillary issues pertaining to E-commerce related cyber crimes, which by implication, includes the issue of cyber privacy.

Thus certain provisions of the Information Technology Act are related to the issue of privacy, though directly The cyber privacy related issues in the IT Act include, unauthorized access, damage to computer through computer contaminants, hacking, breach of privacy and confidentiality and publishing false digital signature certificate for fraudulent purposes etc., Following are some of the related provisions of the Act:

Section 43 of the IT Act deal with the subject of unauthorized access to a person's personal computer which obviously amounts to violation of one's privacy. The section reads : if any person without permission of the owner or any other person who is in charge of a computer, computer or computer network,

1. Accesses or secure access to such computer
2. Downloads, copies ore extracts any data, computer data base or information from such computer
3. Introduces or causes to be introduced any computer contaminant or computer virus into any computer
4. Damages or causes to be damaged any computer
5. Disrupts or causes disruption of any computer
6. Denies or causes the denial of access to any person authorized to access any computer
7. Provides any assistance to any person to facilitate access to a computer
8. Charges the services availed of by a person to the account of another

12 See, PUCL V. Union of India, (1997) 1 SCC 301, Mr. X V. Hospital Z (1998), 8 SCC 296, Sharda V. Dharmpal, (2003), 4 SCC 4931.

person by tampering with or manipulating any computer

He shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

Section 72 of the Act directly deals with 'confidentiality' and 'privacy' of individuals. The section reads : Save a otherwise provided in this Act or other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, or regulation made there under, has secured access to any electronic records, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees or with both.

However, it is obvious from a reading of the section that, it is addressed only the officials who are authorized to collect data under this Act. In its application, this section would be extremely limited since it cover offences only by the authorities such as Adjudication officers etc.,

Further, Section 43-A of the Act imposes a responsibility on the body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resources which it owns, controls or operates to maintain and implement reasonable 'security practices and procedures for protection of such data/information. Any negligence in this regard, resulting in wrongful loss or wrongful gain to any person, such body corporate is liable to pay damages by way of compensation to the affected person.

VII. Violation of Cyber Privacy— Technological Dimensions:

With information and communication revolution making rapid strides in their ambit, the internet has become the fastest growing means of communication through e-mails, chats, browsing etc., there is an increasing reliance on computers concerning all facets of life, coupled with an increasing incidence of cyber crimes, in particular, the violation of right to privacy of individuals, across the globe. However, violation of individual's privacy in the cyber world have no territorial barrier and this makes everything complex as the perpetrators of these crimes are invisible, making the investigation, collection of data and prosecution a more difficult task. As global companies and governments join e-markets places and business becomes borderless, their vulnerability multiplies. Privacy in these e-marketers would be major area of concern in the coming days, with greater degree of damages. Along with these damages there is harassment in several forms to an individual or a group of people online, breaking all barriers of privacy.

Some of the crucial technological operations or acts in the technological front, which pose serious threat to the individual privacy, need special mention.

These include the following:

VII. I. Cookies

A Cookie is information that a Web site puts on one's hard disk so that it can remember something about him at a later time. More technically, it is information for future use that is stored by the server on the client side of a client/server communication.

Cookie activities are on the rise with every passing day and most of the Web sites dealing with e-business are getting technologically smarter, resorting to the practice of collecting the visitors movements to the Web sites. Cookies are used to track people to gain their personal profile and movements, as they go through the Web site. Many users do not go beyond the knowledge that cookies exist and Web sites take advantage of the user's inexperience and collect, catalogue and commodity information totally unwarranted.

The IT Act does not deal with cookies directly. Section 43(b) of the Act says that if any person without permission of the owner or any other person who is in charge of a computer, or computer network downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium, he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person affected. If a Web site sends cookie to a user's machine while he is visiting that Web site without his permission, the Web site could be held liable under section 43 of the IT Act.

VII. II. Web Bug

Web Bug is yet another technical act, which impacts privacy. A Web Bug, also known as a Web beacon, is a file object that is placed on a Web page or in an e-mail message to monitor user behavior, functioning as asking of spyware. Spyware is any technology that aids in gathering information about a person or organization without their knowledge.

Through Web bugs a computer can be subjected to search without following any legal procedure. This is a gross violation of privacy especially at time when a computer has become the storehouse of a person's most valuable information. If a Web bug is planted in a computer without the permission of the owner of the computer, the person responsible for the same is liable to pay damages by way of compensation to the aggrieved person, under section 43 (b) and (c) of the Act.

VII. III. Hacking

Hacking is unauthorized access to a computer and refers to access to the whole or any part of a computer system without permission. Hackers worldwide

attempt to hack into remote computer systems for multiple purposes like eavesdropping, data, data theft, fraud, destruction of data, causing damage to computer systems, or for mere pleasure or personal satisfaction.

Hacking could result in the violation of an individual's privacy and has been made a punishable offence under the IT Act. Section 66 of the IT Act that deals with the hacking states: 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 it 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 fine which may extend up to two lakh rupees or with both.

VII. IV. Spamming

Spamming is another area of concern where cyber privacy is at stake and has become major problem for all internet users. Spam is unsolicited e-mail on the internet and is the internet version of 'junk mail'. Spamming is a weapon to help abusers, who repeatedly bombard an e-mail message to a particular address or addresses. It refers to sending e-mail to hundreds or thousands of users. It is an attempt to deliver a message, over the internet to someone who would not otherwise choose to receive it.

The issue of spamming has not been directly dealt with in any Indian statute. Spam is an unsolicited message requiring one's time and effort to get rid of. A regular supply of such spam messages would naturally result in considerable annoyance. So the law of nuisance under tort law can be used for bringing the spammer to books. Continuous spam could also cause disruption, damage or denial of service to a computer. In case any person is receiving a voluminous , regular supply of spam messages, recourse could be had to section 43(d), (e) and (f) of the IT Act which make damage, disruption to any computer or data or programme illegal.

VII. IV. Data Mining

Data mining is the latest big business in the information age with the rapid developments in the area of information technology, there has been a tremendous expansion in the data bases. 'Data mining' involves classification of the vast computer data for arriving at a meaningful conclusions and using the same for commercial gains i.e., to identify the prospective or potential customers based on the Data mining basements. Innovative organizations are using data mining to locate and appeal to higher value customer, and reconfigure their product offerings to increase their sales. It is needless to state that, data mining amounts to an intrusion into an individual's privacy. Thus, due to the data mining, individuals' privacy is at stake and harassment may continue in different forms.

VII. V. Media and Privacy:

Media has been undoubtedly playing a significant role in our lives. Media has been responsible for bringing the private life of an individual into the public domain and thus exposing him or her to the risk of invasion of his right of privacy. Instantaneous video graphing and photographing and live telecasts by the electronic media of the sensitive private issues, thus disrupting the veil of privacy. As aptly observed by Warren and Brandeis[13], "Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of the home … private devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house tops".

Since freedom of press is a recognized constitutional right, the challenging task in the creation of a full-fledged privacy law is to overcome the difficulty in framing regulations for the media, in a manner, which does not unduly restrict its freedom.

VII. VI. Telephone Tapping:

Telephone tapping is yet another unsolicited and illegal act, which poses a threat to the individual's privacy. With rapid strides made in the information technology, new devices are innovated wherein; telephone tapping by unscrupulous persons and even by the private agencies has become an easier task, thus intruding into the private lives of the individuals, much against the cannons of law. Wiretapping is regulated under the Telegraph Act of 1885. in 1996, the Supreme Court has ruled that wiretaps are a 'serious invasion of an individual's privacy. However, the right is only available and enforceable against the State and not against action by private entities.

VII. VII. Cell Phones— A Threat to Privacy:

The innovation of cell phones, though a technological marvel, enabling instant communication, wherever we are, are proved to be dangerous tools in the hands of mischievous persons, who are using it for commission of various crimes. The modern advanced versions of cell phones, with cameras and videos have become potential tools for the criminals, to intrude into the private lives of people. The increasing incidence of misuse of cell phones has become a cause of constant worry to the protection of privacy of individuals. Added to this, extensive use of cell phones by the business community for the promotion of their products through the forwarding of unsolicited SMS has become a great menace to the individual's privacy.

VII. VIII. Privacy and Medical Science:

Rights of a patient and the need to maintain his privacy has been given

13 Warren and Brandeis, 'The Right to Privacy', 4 Harvard Law Review, 193.

utmost importance in the Hippocratic oath Today any information relating to family's medical records, one's personal preferences, tastes etc, are all vulnerable to storage, meaningful processing and widespread distribution within self-interested circles without any consent. The Hospitals can sell their patient's health records to pharmaceutical companies, which could then target their patients for their medicines. Thus the confidentiality of a patient's health record is at stake. The only permissible disclosure of such a vulnerable record is at the order of a court or in the cases where 'public interest' overrides the duty of 'confidentiality'.

Some of the other crucial issues pertaining to the health privacy are the new techniques developed in the medical field pertaining to the medically assisted reproductive techniques like IVF, storage of Genetic information etc.,

From the above discussion, it becomes clear that, modern technological and electronic devices and their operations have great potential to intrude into the right to privacy and that the existing legal frame work is quite inadequate to address the privacy issues emanating from them.

VIII. Protection of Cyber Privacy in the Electronic Age— The Way Ahead:

The right to privacy is under utmost threat in the present age of technological development, than ever before. Unfortunately, the legislators have turned a blind eye towards the problems and have shown scarce concern towards the issue. Though the courts in India have granted the citizens the right to protect their privacy but the attitude of the legislature and the executive have been very regressive and far from satisfactory. No right can be enjoyed in the true sense unless and until there are instruments to protect those rights. Unless and until the state comes forward to protect the right of privacy, there is no personal sphere and space left for the individuals to exercise his right to free speech and expression, without any fear of intrusion.

With the recent development of commercially available technology based systems, privacy has also moved into the hands of individual users. It is pertinent to note that, the larger issue of online privacy remains unaddressed in the Indian IT Act, which implies that, the victims of violation of cyber privacy are almost without any effective remedy. Though several international legal instruments seek to protect right to privacy as a human right, there is hardly an efficacious mechanism at the global level to enforce the same, considering the fact that, cyber privacy has no geographical boundaries and it involves larger issues like, jurisdiction, conflict of laws etc.,

In sum, it may be concluded that, advancements made in the field of communication and technology are slowly but steadily turning to dominate and encroach into almost every facet of the people's lives. George Orwel's fear that advanced technologies would be used to monitor the people in all their endeavours is a reality now in this era of information and communication revolution and

surely, these fears are going to engulf us more, if proper resistance is not adopted through legislations and a concerted efforts on the part of the international community in the ultimate interest of protecting the people's privacy, which is a paramount human right.

It is high time that legislative and policy measures are initiated by the government and the international community at large, to curb the increasing incidence of abuse of modern technologies and ensure the securing of fundamental right to privacy of an individual. In this direction following suggestion are made:

1. A national level monitoring body should be created to monitor and supervise the functioning of the internet systems in the country
2. Crimes committed in the cyber space, more particularly, involving the privacy should be governed by the principles of 'universal jurisdiction' to bring the offenders to book, as in the case of pirates.
3. A comprehensive international agreement should be entered into by the States for effective enforcement of cyber related legislations, as cyber space is devoid of boundaries.
4. Measures should be taken to adopt the Guidelines provided by the OECD on the Protection of Privacy and Trans-boundary Flow of Personal Information.
5. The enforcement machinery pertaining to the cyber crimes should be well trained and well equipped to nab the cyber criminals who are intruding into the private lives of individuals.