12.1 Concluding Remarks

Alan Westin said that the concept of “Privacy” is not alien to any specie on this planet. Anthropological studies have proved that men and animals do share several basic mechanisms for claiming privacy among their own fellows.\(^1\) However, it is submitted that human beings are blessed with some extraordinary senses, and have been fighting for preserving their ‘privacy rights’ since times immemorial. Aptly, David Flaherty argues that the concept of ‘privacy’ has its antecedents in ‘ancient times, biblical literature, and Roman law.’\(^2\) To support this argument, Milton Konvitz explains that the first page of the Bible introduces the feeling of shame as a violation of privacy.\(^3\) After Adam and Eve had eaten the fruit of the tree of knowledge, “the eyes of both were opened, and they knew that they were naked; and they sewed fig leaves together and made themselves aprons.”\(^4\) Mythically, it has been observed that our very knowledge of good and evil is linked with a sense and realm of privacy.\(^5\)

Similarly, ancient scriptures proved that there was a difference between public and private sphere in the ancient Greece. In this era the word for private was \textit{idios}, meaning ‘one’s own, pertaining to one’s self’, hence private or personal. The word for public was used as \textit{Koinos}, which means ‘common’ in the sense of shared in common as opposed to private.\(^6\) The noun form of \textit{idios} is \textit{idiotes}, from which comes the English word ‘idiot’. Its main meaning is a private person or individual, or one in a private station as opposed to one holding public office or taking an active part in public affairs. It can also mean a layman or person lacking professional knowledge and by extension, an ignoramus or raw hand.\(^7\) Jurgen

\(^7\) Ibid.
Habermas also noted that the sphere of the *polis* was strictly separated from the sphere of the *oikos* i.e the private sphere of an individual.\(^8\)

For Aristotle the *oikos* was a private sphere attached to the home, namely the private household. Thus family life served as a paradigm of the private sphere that defined the role of women. A male citizen’s status in the *polis* depended on his unlimited and dominant status as master in the *oikos*.\(^9\)

It is submitted that every society, clan, tribe, community or class do maintain certain minimum standards for preserving their private lives, cultures and traditions. They value the importance of privacy. Thus, it is incorrect to say that the concept of ‘privacy’ is a pure invention of the modern legal system. Barrington Moore, Jr., analysed the study of a remote Eskimo community of twenty to thirty-five people living inside the Arctic Circle. This qualitative study was done by Jean L. Briggs.\(^{10}\) Even under difficult conditions, as Briggs observed, the Eskimos have very strong sense of privacy with regard to their thoughts, their feelings, and motivations. This sense of privacy is due to maintain social harmony among community. In primitive societies a man who was truly alone when he was away from fellow humans was a man in terrible peril, since hostile spirits were believed to be all around- in the bodies of animals, in trees or rocks, in shadows, and even in the air.\(^{11}\)

Again, needs for privacy do also appear in the intimacy of sexual relations. There are only a few exceptions to the norm that men and women will seek seclusion for performance of the sexual act. Only in a few cultures, such as the Formosan and among Yap natives of the Pacific, is the sexual act performed openly in public. Even here, Formosans will not have intercourse if children are present and Yapese couples are generally secluded when intercourse takes place, though they do not seem to mind the presence of other persons who may come on the scene.\(^{12}\)

Furthermore, the roots of the concept of right to privacy were also traced back into the ancient principles of the common law. In earliest times, the common law was confined only to protect one’s life and property from physical interference. With the passage of time, however, the great shifts took place which started recognising intangible, incorporeal,

---

\(^8\) Jurgen Habermas, *The Structural Transformation of the Public Sphere*, 3 (1989).
\(^{10}\) Supra note 6 at 3.
\(^{11}\) Supra note 1 at 18.
\(^{12}\) Id., at 14.
spiritual values. It was realized that the right to life includes the right to enjoy life. Similarly, it was recognized that a real injury to human sensibilities could be inflicted when one is merely placed in imminent danger of battery by an attempt at bodily harm. In 1348 or 1349, therefore, the first recovery for civil assault was granted. People started giving value to their reputation and their honor as well as their skins. Consequently, the common law recognised the recovery in case of slander. Finally, one’s thoughts, emotions, sensations and spirituality were legally recognized under common law.

Increasingly, the growth of ‘privacy’ got its momentum in 1765 when British Lord Camden, struck down a warrant to enter a house and seize papers. Parliamentarian William Pitt wrote, ‘The poorest man may in his cottage bid defiance to all the force of the Crown. It may be frail; its roof may shake; the wind may blow through it; the storms may enter; the rain may enter-but the King of England cannot enter; all his forces dare not cross the threshold of the ruined tenement.’

However, we had to rely on the history of privacy in the United States for understanding the modern concept of privacy. In United States, the modern concept of the right to privacy has been developed by the courts. In United States, when the Constitution and Bill of Rights were ratified, neither statutes nor common law rules established a right of privacy as such. The debate on the law of privacy got ignited with the publication of an article written by Samuel D. Warren and Louis D. Brandeis in 1890. Out of a few fragments of the common law, the authors invented a brand new tort, the invasion of privacy. Dean Roscoe Pound reportedly said that the article did nothing less than add a chapter to the law.

Warren and Brandeis noted that the technological equipments had potential to invade our privacy. Warren and Brandeis defined privacy as the ‘right to be let alone,’ a phrase

---

15 Year Book, Lib. Ass., Folio 177, pl. 9, cited Pollock and Maitland, The History of English Law, 536 (1911).
18 M. Glenn Abernathy, Civil Liberties under the Constitution, 94 (1977).
19 Id., at 95.
adopted from Judge Thomas Cooley’s famous treatise on torts in 1880. Cooley’s right to be let alone was, in fact, a way of explaining that attempted physical touching was a tort injury; he was not defining a right to privacy. Warren and Brandeis’s use of the phrase was consistent with the purpose of their article: to demonstrate that many of the elements of a right to privacy existed within the common law.  

The authors declared that the underlying principle of privacy was ‘that of inviolate personality.’ They noted that the value of privacy is found not in the right to take the profits arising from publication, but in the peace of mind or the relief afforded by the ability to prevent any publication at all. Warren and Brandeis observed that privacy invasion by new technologies would cause mental pain and distress to an individual, which is far greater than bodily injury. The authors noted that this type of harm was not typically protected by tort law. While the law of defamation protected injuries to reputations, privacy involved ‘injury to the feelings’, a psychological form of pain that was difficult to translate into the tort law of their times, which focused more on tangible injuries.

Later on, when Louis Brandeis became a justice of the United States Supreme Court, he wrote his famous dissenting opinion in the case of *Olmstead v. United States.* In this case, the majority held that wiretapping was not a violation under the Fourth Amendment because it was not a physical trespass into the home. But Louis Brandeis refused to accept the majority decision and wrote his dissenting opinion. He said that the Framers of the Constitution did not intend to give narrow interpretation to the Fourth Amendment of the United States Constitution. Rather the Constitution makers intended to confer such valuable right against the government.

Finally, Brandeis’s article and his dissent inspired all subsequent developments in law of privacy. In *Katz v. United States,* the Court adopted Brandeis’s dissenting view, and overruled its earlier judgment. In its Fourth Amendment jurisprudence, as well as its substantive due process protection of the right to privacy, the Court frequently has invoked Brandeis’s formulation of privacy as the right to be let alone.

---

22 Supra note 20 at 1100.
23 Supra note 21 at 205.
24 Id., at 200.
25 Id., at 196.
26 Id., at 197.
27 277 U.S. 438 (1928).
28 Id., at 478.
30 Supra note 20 at 1101.
Warren and Brandeis’s aim was to explore the roots of a right to privacy in the common law and explain how such a right could develop. Consequently, a law of privacy gradually developed by statute and by common law decision in state courts. But it was not until 1965 that the United States Supreme Court squarely held that the Constitution contained at least a limited right to privacy. The United States’ courts have developed privacy right on a constitutional basis. Various amendments of the American Constitution like first, fourth, and fifth, containing provisions protecting privacy interests has laid the necessary foundation for the courts in this regard. These amendments mainly protect informational privacy. The privacy regarding decisional privacy was protected mainly using the ninth amendment. Evolution of privacy as a constitutional right in America was through cases which fell in categories of (1) sexuality (2) search and seize (3) eavesdropping (4) Data protection and press.

Besides, the law of privacy has been developed through many philosophical debates. Many authors, who believe in the universal value of the concept of privacy, say that it is very difficult to define privacy as it varies by socio-historical contexts. For comprehensive understanding, the literature on privacy has been divided into two main categories i.e. reductionism and coherentism. Reductionists are those authors who criticise the concept of privacy. And Coherentists defend the coherent values of the concept of privacy. "Reductionists" argue that there should not be a distinct legal right to privacy because the right to privacy is always derived from other rights like the rights to property, to liberty, or over one’s person. On the contrary, coherentists believe in the fundamental, distinctive and coherent characteristics of various claims that have been called privacy interests. However, there are divergent views among the coherentists also.
Considering philosophical debates, we observed that the scope of the concept of privacy is very wide in nature. Besides, the United States Supreme Court claimed in *Whalen v. Roe*,\(^{40}\) that there are two different dimensions to privacy i.e. both control over information about oneself and control over one’s ability to make certain important types of decisions. The Court defined the right to privacy, embracing both an individual interest in avoiding disclosure of personal matters and an interest in independence in making certain kinds of important decisions.\(^{41}\) Finally, as the researcher observed, number of theorists adopted the court’s reasoning and, admitted that the concept of privacy has a very wider scope which includes multiple types of privacy issues. For example privacy includes control over information about oneself, control over access to oneself, both physical and mental, and control over one’s ability to make important decisions about family and lifestyle in order to be self expressive and to develop varied relationships.\(^{42}\) Furthermore, privacy values are also the basic pillars of our democratic set up since privacy ensures one’s speech and expression, and provides autonomy over one’s personal decisions. In addition to this, privacy enhances social interaction on a variety of levels. For Daniel J. Solove, a society without privacy is a ‘suffocating society’.\(^43\)

At the international level, the United Nations give recognition to the right to privacy through many conventions like Universal Declaration of Human Rights, 1948, which specifically protects territorial and communications privacy. Article 12 of the Universal Declaration of Human Rights (1948) protects individuals’ privacy, honour and reputation, their families, home, and correspondence against any arbitrary interference.\(^44\) Article 17 of the International Covenant of Civil and Political Rights\(^45\) (to which India is a party), contains the same wordings and protects everybody’s privacy. The right to privacy is also dealt with in various other international instruments, such as the United Nations Convention on the Rights of the Child, the International Covenant on Civil and Political Rights (ICCPR), and the

\(^{40}\) 429 U.S. 589 (1977).
\(^{41}\) *Id.*, at 598-600.
\(^{42}\) *Supra* note 9 at 73.
\(^{43}\) *Ibid.*
\(^{44}\) The Universal Declaration of Human Rights, 1948, Art. 12.
It provides as follows:
“No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”
\(^{45}\) The International Covenant of Civil and Political Rights, Art. 17.
It provides as follows:
“1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.”

Furthermore, the European Convention on Human Rights gives full respect to one’s private and family life, and allows public authority’s interference only under exceptional circumstances. It represents that right to privacy is not absolute right and, the public authority can interfere one’s private life in the interests of national security and public safety. Similarly, privacy rights are not available by jeopardizing others’ health, morals, rights, and freedoms.\(^{47}\)

Besides, the European Court of Human Rights has also played a significant role in giving universal recognition to the right to privacy. The European Court in \textit{Gaskin v. United Kingdom},\(^{48}\) following the death of his mother, the applicant was received into care by a local authority. He ceased to be in the care on attaining the age of majority. In the period during which the applicant was in care, he was boarded out with various foster parents.\(^{49}\) He contends that he was ill-treated.\(^{50}\) The applicant, wishing to bring proceedings against the local authority for damages for negligence, made an application for discovery of the local authority’s case records made during his period in care. Discovery was refused by the High Court on the ground that these records were private and confidential.\(^{51}\) Finally, the European Court opined that persons in the situation of the applicant have a vital interest, protected by the Convention, in receiving the information necessary to know and to understand their childhood and early development.\(^{52}\)

It provides as follows:

1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.
2. The child has the right to the protection of the law against such interference or attacks.”

\(^{47}\) The European Convention on Human Rights, Art. 8.
It provides as follows:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority except such as is in accordance with law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the protection of health or morals or for the protection of the rights and freedoms of others.

\(^{48}\) Application no. 10454/83, Judgment from the European Court of Human Rights, Strasbourg, 7 July 1989.
Available at http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57491#{"itemid":"001-57491"} accessed on July 20, 2013, at 4:00 p.m. IST.

\(^{49}\) Id., paragraph 10.

\(^{50}\) Id., paragraph 11.

\(^{51}\) Id., paragraph 14.

\(^{52}\) Id., paragraph 49.
Furthermore, the Canadian Charter of Rights and Freedoms recognizes everyone’s right to life, liberty and security.\(^{53}\) It also provides that everyone has the right to be secure against unreasonable search and seizure.\(^{54}\) Similarly, the New Zealand Bill of Rights declares in section 21 that everyone has the right to be secure against unreasonable search or seizure, whether of the person, property or correspondence or otherwise.\(^{55}\)

So far as the data privacy is concerned, the Directive 95/46/EC of the European Parliament is a backbone of European Union (EU) data privacy protection laws. The Directive of 1995 was laid down for the protection of individuals with regard to the processing of personal data and on the free movement of such data. The motive of the Directive was to develop economic growth, while protecting European Union’s citizens’ privacy.\(^{56}\) It was intended that there should be a free flow of personal data within European Union member countries, while affording the privacy protections to the citizens. It means that protection will be provided to the citizens’ personal data even outside of European Union member countries. Furthermore, personal data is barred from transferring to a third country who doesn’t have an adequate law on privacy protections.\(^{57}\) For example, a business traveler from a country without adequate protection may not take data about business or customer contacts collected in European Union member countries outside the European Union. By barring the transfer of personal data from European Union citizens to businesses and other entities in countries without levels of privacy protection deemed appropriate by the European Union, the directive sets de facto standards for data protection internationally. Accordingly, countries such as Canada, Australia, and Japan have implemented data protection laws that provide similar levels of protection for personal data. Others-in particular the United States-

\(^{53}\) Canadian Charter of Rights and Freedoms, Section 7. Available at http://laws-lois.justice.gc.ca/eng/Const/page-15.html#h-44 accessed on July 20, 2013, at 4:00 p.m. IST. It provides as follows:
“Everyone has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice.”

\(^{54}\) Id., Section 8. It provides as follows:
“Everyone has the right to be secure against unreasonable search or seizure.”

\(^{55}\) New Zealand Bill of Rights Act 1990, Section 21. Available at http://legislation.govt.nz/act/public/1990/0109/latest/whole.html#DLM225523 accessed on July 20, 2013, at 4:00 p.m. IST. It provides as follows:
“Everyone has the right to be secure against unreasonable search or seizure, whether of the person, property, or correspondence or otherwise.”


have worked out special agreements with the European Union so that United States businesses can claim compliance with these principles.\(^58\)

The Directive considered the right of individuals to control the collection, distribution, and use of their personal information as a traditional human right, which can be protected only by implementing ‘fair information practices’ i.e. principles of openness, access and correction, collection limitation and finality, accuracy, security, and enforcement or redress.\(^59\) In 2010, European Commission’s Communication entitled, “A comprehensive approach on personal data protection in the European Union,” revised the existing European Union (EU) data protection directives to check its validity in the technological world. It was stated that Directive of 1995 is historical document in the field of data protection in the European Union. It was born with two objectives i.e. the protection of personal data, on the one hand, and the free flow of personal data for economic growth, on the other. After conducting thorough research, it was concluded by the Commission that the objectives and the principles enshrined in the Directive remain valid.\(^60\)

However, the European Commission noticed that technological advancements have brought new challenges for protecting one’s personal data. The commission observed that technology and social networking sites have made easy for the individuals to share personal information publicly and globally. This sharing of personal information leads to ‘Cloud computing’, which is being considered as a serious challenge to data protection. In such phenomenon, the individual loses control over his sensitive information.\(^61\)

Recently, on 25\(^{th}\) January 2012, European Commission’s Communication gave a proposal on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. Article 1(7) of the proposal provides that high level of protection of the personal data of individuals and facilitating the exchange of personal data between competent authorities of Members States is necessary for effective judicial co-operation in criminal matters and police cooperation. Therefore, in order to achieve this end, the level of protection of the rights and freedoms of individuals with regard to the processing of personal data by competent


\(^{59}\) \textit{Id.}, at 208.


\(^{61}\) \textit{Ibid.}
authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties must be equivalent in all Member States. Effective protection of personal data throughout the Union requires strengthening the rights of data subjects and the obligations of those who process personal data, but also equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data in the Member States.62

Although there is no general right to privacy in the United Kingdom, the courts have developed the right to privacy by recognising the rule of breach of confidence63 But significant changes were brought up by the implementation of the Human Rights Act 1998 (the HRA), which incorporated into United Kingdom law the European Convention of Human Rights (the Convention). With the global spread of information, it is also impossible to ignore the rulings of the European Court of Human Rights (ECHR), whose long fingers probe the domestic laws of every member country.64 Lord Nicholls said in *Campbell v. MGN*,65 that the protection of various aspects of privacy is a fast developing area of the law in the common law jurisdictions. Indeed, in *Douglas v. Hello! Ltd*66 and *Von Hannover v. Germany*,67 it was declared that the courts have a duty to recognise and protect privacy rights.

The British Parliament also approved the Data Protection Act in July 1998 to implement the European Union Data Protection Directive. The legislation, which came into force on March 1, 2000, applies to records held by government agencies and private entities. It creates eight data protection principles based on the Directive to be followed. These provide for limitations on the use of personal information, access to, and correction of, records, adequate security, and requires that entities that maintain records register with the Information Commissioner.68

Against the phone-hacking scandal in England, Justice Leveson has submitted its report. Justice Leveson found that the current systems of both internal governance in some

---

66 (2003) 3 All E.R. 996
parts of the press, and industry self-regulation of the press are not working properly.\textsuperscript{69} The present Press Complaints Commission (PCC) lacks the independence that is critical to building public confidence in a regulator.\textsuperscript{70} Justice Leveson envisaged that the industry should come together to create, and adequately fund, an independent regulatory body, headed by an independent Board, that would: set standards, both by way of a code and covering governance and compliance; hear individual complaints against its members about breach of its standards and order appropriate redress; take an active role in promoting high standards, including having the power to investigate serious or systemic breaches and impose appropriate sanctions; and provide a fair, quick and inexpensive arbitration service to deal with any civil complaints about its members’ publications.\textsuperscript{71} Justice Leveson further recommended that the standards code must ultimately be the responsibility of, and adopted by, the Board advised by a Code Committee which may comprise both independent members of the Board and serving editors. It was, therefore, recommended that the Code must take into account the importance of freedom of speech, the interests of the public (including the public interest in detecting or exposing crime or serious impropriety, protecting public health and safety and preventing the public from being seriously misled) and the rights of individuals. Specifically, it must cover standards providing for conduct, appropriate respect for privacy, and accuracy, and the need to avoid misrepresentation.\textsuperscript{72}

It has been observed that an individual’s right to privacy always gets affected whenever he or she is subjected to surveillance. Increasingly, the government’s monitoring ability has become more powerful than ever in the current technological world.\textsuperscript{73} And people have been justifying the government’s surveillance power since 9/11 attacks in United States and 26/11 attacks in Mumbai. It reflects people’s belief and trust in the government’s programmes of collecting personal details. However, the misuses of individuals’ personal information for unlawful purposes and excessive use of surveillance technologies have disturbed the equilibrium of privacy, disclosure, and surveillance.\textsuperscript{74}

At the same time, the impact of surveillance on human behavior cannot be ignored. If surveillance does not provide necessary space to a person for his actions and thoughts, he

\textsuperscript{70} Id., at 1749.
\textsuperscript{71} Id., at 1759.
\textsuperscript{72} Id., at 1763.
\textsuperscript{73} Christopher Slobogin, Privacy at Risk, 3 (2007).
\textsuperscript{74} Daniel J. Solove, Nothing to Hide, 2 (2011).
would face certain schizophrenic implications. Indeed, privacy is definitely required for the
effective operation of social structure. Only those who can sustain an absolute commitment
to the ideal of perfection can survive total surveillance. However, this is not the condition of
men in ordinary society. Furthermore, an individual has right to disclose secrets about his
soul or personality to whom he likes. But compulsion to reveal those parts of his memory and
personality that he regards as private, amounts to violation of person’s psychological
privacy. It is believed that there is a total loss of privacy in ‘total institutions’ like prisons,
asylums, hospitals, etc. Describing the situation in Asylums, Erving Goffman observed that in
total institutions the basic components of the self like thoughts, emotions, actions, etc. are
violated.

Increasingly, government’s extensive collection of personal information interferes
with an individual’s freedom of association, right to speak freely, right to speak
anonymously, etc. Therefore, in such situations, a dissenter might feel an apprehension of
being identified, and falsely prosecuted. These types of harms can inhibit individuals from
associating with particular people and groups and from expressing their views, especially
unpopular ones. This kind of inhibition is a central goal of Orwell’s Big Brother. Although it
certainly does not approach the same degree of oppressiveness as Big Brother, it reduces the
robustness of dissent and weakens the vitality of our communication.

Alan F. Westin, aptly, observed that in the period of limited information technology,
people supported and participated in the information collecting processes. However, the
government’s unjustifiably excessive surveillance, through advanced physical, psychological,
and data surveillance technologies, has alarmed the society to show their concern towards
privacy rights.

Increasingly, almost every private sector is using technologies and softwares to make
their own proprietary databases. These databases have information for many variables on
many people, and it is possible to look for useful correlations. Companies collect data about

---

75 Supra note 1 at 58.
76 Id., at 59.
77 Id., at 61.
American Philosophical Quarterly, Vol. 24, No. 1 (Jan., 1987), 81-89 at 83. Available at
on July 19, 2011, at 1:30 p.m. IST.
81 Id., at 436.
82 Renee Marlin-Bennett, Knowledge Power, 151 (2004).
customers, their own products, their employees, or the companies they do business with.\textsuperscript{83} The interesting aspect is that the information itself has become a valued property. The value is in the information it contains like potential customers’ names and their addresses. Today, computers are able to combine large datasets into a single database that can be mined to extract commercially useful information.\textsuperscript{84} Therefore, the commodification of information and the ability of computers to manipulate informational data has become potential threat to individual privacy.

So far as India is concerned, the concept of privacy has its root in ancient times. The religious scriptures also recognize the concept of privacy as a sacred one. The impact of individualism was felt in India only towards the close of nineteenth century. The break-up of the joint family is due to several causes. For education young men and women have to separate themselves from the family to live in university centres. Occupation often forces the members of the family to live separately in distant places. Legislative reform has led to the division of property among the members of the family. Sometimes lack of adjustment compels couples to break away from the joint family.\textsuperscript{85}

Inspite of the criticism, the joint family system prove itself to be the best social institution. Young children living in a joint family develop a group consciousness and show greater cooperativeness and spirit of self-sacrifice.\textsuperscript{86} Joint family system still has strong roots in the Indian society. The interdependence, love, affection and care, for each other, promote the security, both physical and psychological, among the family members. Indian joint families have their own set of standards for preserving family privacy, community privacy, and group privacy and so on. Ultimately, the society as a whole respects such rites, ceremonies and norms set for the family privacy. In the Indian joint family system the leader of the family, known as \textit{Karta}, is responsible for all needs of the family. He takes care of every individual member. He is very much cautious about the family privacy and does not let anything publicize due to which the family’s reputation would have been at stake. The family members settle their sensitive matters by their own. Again if the matter goes more serious, then the whole village or community settles it for the sake of village reputation.

The researcher analysed that the ‘privacy values’ had been embedded in the Indian religious scriptures, architectural models of ancient houses, etc. Besides, privacy has also been observing as a customary right since ancient times. Right to privacy was initially

\textsuperscript{83} Id., at 163.
\textsuperscript{84} Id., at 164.
\textsuperscript{86} Id., at 67.
practiced as a custom. Among various customs, there was the norm of the seclusion of women from the male stranger’s gaze. This custom of privacy had its foundation laid in the rules regulating the construction of houses. The earliest mention of such rules is found in the Kautilya’s *Arthashastra* wherein the violation of such rules was made punishable.\(^{87}\)

British regime did realize the importance attached to the customs by the Indians. Moreover, during the British period, the courts focused on the individual legal rights in India.\(^{88}\) During British period, the courts discovered the customary right of privacy from various property rights. At that time, there was no common law tort of invasion of privacy in England. And there was no general right of privacy existed in statutory form. Lord Camden C.J. in *Entick v. Carrington*\(^{89}\) said that the eye cannot by the laws of England be guilty of a trespass. It was argued that just as the law of easements does not protect any right to a good view or prospect, there is likewise no easement of indefinite privacy. There was, in general, no common law right to resist having one’s land and one’s activities on that land overlooked by one’s neighbours or indeed by others. But it was observed that in the different cultural climate of certain parts of British India during the 19th century customary law intervened to prevent the overlooking of land where otherwise the privacy and seclusion of *pardanashin* women would have been threatened.\(^{90}\)

The customary right of privacy got its statutory recognition in the Indian Easements Act, 1882. The contents of this customary right, by and large, are mainly concerned and centered around the complaints regarding the construction of a new house or alteration of the old ones, opening a new door or a window or enlargement of the existing ones, construction of a new floor or balcony and opening of a new aperture or the enlargement of the old ones by the defendant whereby the plaintiff’s house specially that portion of the house which is generally secluded from observation and/or inhabited by the female members of his/her family, is exposed to the view of the defendant resulting in an invasion of the plaintiff’s privacy.\(^{91}\)

\(^{87}\) G. Mishra, *Right to Privacy in India*, 82 (1994).
\(^{89}\) (1765) 19 Howell’s State Trials 1029, 1066.
\(^{91}\) Supra note 87 at 83.
In *Mohomed v. Birju Sahu* 92, it was said that to hold privacy a natural right would lead to the most alarming consequence to the owners of the house property in cities since, by erecting female apartments, a man could prevent his neighbours building as they wished and the erection of such apartments by a few persons might render all the surrounding land useless for habitation.93 Nevertheless in a number of cases the High Courts of Allahabad, Bombay and Calcutta held that such a right of privacy can be acquired by prescription, grant or custom.94

There was no specific discussion on the concept of privacy in the Constituent Assembly Debates. In Post-independence Era, it was mainly the judiciary who played significant role in the making of fundamental right to privacy. In India, the judiciary derived the right to privacy from various fundamental rights like freedom of speech and expression, and right to life and personal liberty, mentioned under the Constitution of India.95 Similarly, the Indian judiciary considered phone tapping as a serious invasion of one’s right to privacy. Such argument is based on the principle that the ‘State’ cannot impose unreasonable restrictions on one’s right to life or personal liberty. In *People’s Union for Civil Liberties v. Union of India*,96 the Supreme Court held that wiretapping is a serious invasion of an individual’s privacy. The court observed that telephonic conversation is a part of a man’s private life. And certainly, right to privacy includes telephonic conversation in the privacy of one’s home or office. Thus, telephone tapping under S. 5(2) of Telegraph Act, 188597 would violate an individual’s right to privacy unless it is permitted under the reasonable procedure

---

93 Ibid.
96 (1997) 1 SCC 301.
97 The Indian Telegraph Act, 1885, s. 5(2).

It provides as follows:

“On the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorised in this behalf by the Central Government or a State Government may, if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offence, for reasons to be, recorded in writing, by order, direct that any message or class of messages to or from any person or, class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order: Provided that press messages intended to be published in India of correspondents accredited Central Government or a State Government shall not be intercepted or detained, unless their transmission has been Prohibited under this sub-section.”
established by law. For this, the court laid down certain guidelines to regulate the government’s action of wiretapping. It was directed by the Hon’ble Supreme Court that the interception order shall be issued by the Home Secretary, Government of India (Central Government) and Home Secretaries of the State Governments. It is also required that copy of such order shall be sent to the Review Committee within one week. The order should contain every detail of the whole mechanism of interception. Name of the person to whom the order is addressed and, the person to whom intercepted information is being disclosed should be mentioned in the respective orders. The validity of the order can also be checked on ground, whether the information could reasonably be acquired by other means or not. Thus, it is necessary that reasons should be recorded before issuance of the orders. Furthermore, the order shall, unless renewed, cease to have effect after two months. The total period for the operation of the order shall not exceed six months. The issuing authority shall also maintain the records of intercepted material like for what purpose message was intercepted, which telecommunication device was intercepted, how the intercepted material was used, to whom it was disclosed, and what is the number of copies, made of intercepted material. The intercepted material should only be used for that purpose for which it was intercepted. More importantly, every copy of the intercepted material should be destroyed if the purpose has been achieved.

In District Registrar and Collector v. Canara Bank,98 the court struck down Sec. 73 of the Indian Stamp Act, 1899 as amended by the Andhra Pradesh Act (17 of 1986) as permitting an overbroad invasion of private premises or the homes of persons in possession of documents in a power of search as seizure without guidelines as to who and when and for what reasons can be empowered to search and seize, and impound the documents. The Court held that the right to privacy dealt with persons and not places. The court, however, held that no right to privacy could be available for any matter which is part of public records including court records.

Recently in Selvi v. State of Karnataka99, the Supreme Court held that compulsory administration of any of the techniques, like narcoanalysis, polygraph examination and brain Electrical Activation Profile(BEAP) test, is an unjustified intrusion into the mental privacy of an individual.100 It was also recognized that forcible intrusion into a person’s mental

---

98 (2005)1 SCC 496.
99 2010(4) SCALE 690.
100 Id., at 783.
processes is also an affront to human dignity and liberty, often with grave and long-lasting consequences.\(^{101}\)

In *Re: Ramlila Maidan Incident Dt. 4/5.06.2011 v. Home Secretary, Union of India and others,*\(^{102}\) decided on 23 February, 2012, the Supreme Court noted that even if the assembly was illegal, the action of police under Section 144 Cr.PC without being preceded by an announcement to the sleeping individuals was not reasonable. The court observed that ‘Sleep’ is a basic requirement for the survival of every human life. Furthermore, to disturb someone’s sleep is a violation of his or her human right as it amounts to torture. Therefore, the court declared that right of privacy of sleeping individuals was immodestly and brutally outraged by the State police action.\(^{103}\)

The Supreme Court of India have also started recognizing the one’s decisional privacy rights. The Delhi High Court in *Naz Foundation v. Government of NCT of Delhi,*\(^{104}\) declared that Section 377 IPC, insofar it criminalises consensual sexual acts of adults in private, is violative of Articles 21, 14 and 15 of the Constitution. While giving more and more personal autonomy to the individual, the Supreme Court in *S. Khusboo v. Kanniammai,*\(^{105}\) recognized the Live-in relationships, as one’s decisional privacy. The court held that there is no statutory offence that takes place when adults willingly engage in sexual relations outside the marital setting, with the exception of adultery as defined under Section 497 IPC. Furthermore, the court observed that notions of social morality are inherently subjective and the criminal law cannot be used as a means to unduly interfere with the domain of personal autonomy.

But Indian Courts have not yet laid down any clear cut principles on the subject of “Sting Operation” However, we have certain principles like public interest may override one’s right to privacy and liberty. The illegality inherent in the publication/exhibition of fabricated and misleading content obtained by Sting Operation which is universally condemned is recognized by the courts in India.\(^{106}\) In the absence of any strict regulation, the principles of self regulation in journalism are of worth mentioned over here. Few of them are like sting and undercover operations should be a last resort of news channels in an attempt to give the viewer comprehensive coverage of any news story, news channels will not allow sex and sleaze as a means to carry out sting operations, the use of narcotics and psychotropic

\(^{101}\) *Id.,* at 778
\(^{103}\) *Id.,* at 248.
\(^{104}\) 2010 Cri. L. J. 94 (Del.).
\(^{105}\) (2010) 5 SCC 600.
\(^{106}\) www.lawcommissionofindia.nic.in/stingoperation.doc accessed on December 4, 2010 at 11.48 p.m. IST.
substances or any act of violence, intimidation, or discrimination as a justifiable means in the
recording of any sting operation, etc.  

Similarly, irresponsible media intrudes into celebrities’ privacy for reporting
sensational and salacious news. Sensational and salacious gossips serve no public interest. In
*Von Hannover v. Germany*, paparazzi took pictures of Princess Caroline of Monaco, the
eldest daughter of Prince Rainier III of Monaco, which were completely of private nature.
Thus, it is important to note that instead of looking to physical zones when determining
privacy (i.e., a public or private place), the court determined that certain activities can be
exclusively private. The focus is then on the subject matter of the photographs rather than the
location where they were taken.  

Currently, it has been observed that the social networking sites are also being used for
stalking or other illicit monitoring of users’ physical movements, and subjecting children to
many abuses. Moreover, the users are ill informed and unaware about the processing of their
personal information. The increased use of social network sites has led to increased
concerns about users’ privacy not only in terms of the data collected and used by the
organization but also in light of the possible impact of mass sharing of personal information
on social relations.  

12.1.1 Important Findings of Data Analysis

Following are some important findings of the data analysis:

- Substantial portion of population in Chandigarh are unaware of right to privacy.
- In India, right to privacy has been developed in a very limited sense only.
- In India, law is unclear on public officials’ right to privacy. Moreover, due to
  lack of awareness the public information officials (PIOs) face many practical
difficulties in deciding public officials’ right to privacy.

---

108 *Supra* note 67.  
109 Id., at 66.  
110 Shannon Vallor, "Social Networking and Ethics", in Edward N. Zalta (ed.), The Stanford Encyclopedia of
111 David J. Houghton & Adam N. Joinson, “Privacy, Social Network Sites, and Social Relations, Journal of
• Due to inefficiency and insufficiency of rules and regulations, the Sting Operations are being conducted in unregulated manner.

• In the field of journalism, an unhealthy competition and exploitative environment compels journalists to report sensational and indecent news by violating individuals’ right to privacy.

• At many places, the researcher found that newspapers and Television news channels have appointed unqualified and ineligible journalists, who hardly sensitized towards individuals’ privacy. In addition to this, they even don’t know about any media ethics.

• Individual users of Social Networking Sites are unaware of the advanced privacy settings available on these sites.

• The social networking sites do not take informed consent from its users while processing their users’ personal information.

• There are no comprehensive policies or rules or regulations on social media.

• There is very less judicial scrutiny of these social networking sites in India.

• Parents have no control over their Children’s internet accesses because of parents’ unawareness or illiteracy or both. Therefore, they are using internet, mobile phones, etc. without any sense of responsibility.

• Since India has insufficient treaties on data protection with foreign countries, Indian officials dealing with cyber crimes face difficulties in tracing online abusers' servers, situated outside India.

• The law enforcement agencies have got extensive powers to access online users’ personal information.

• In many cases, it has been seen that the executive agencies compel the social networking sites to provide them easy access to the users’ personal information. Increasingly, the social networking sites have reported in many cases that they are being compelled by the executive agencies to remove that content or material from their websites which is against their political ideology or any policy. In this sense, it is violation of one’s freedom of speech and expression.

• The prevailing legislations are insufficient and inefficient to regulate closed circuit television (CCTV) cameras monitoring. In most of the cases, camera
control operators are not educated culturally, morally, ethically, technically and legally.

- The mobile camera users are not sensitized towards individuals’ privacy. It is because of non-availability of any code of conduct.
- Biometric identification system requires more clarity. Since there is no comprehensive legislation on data protection, biometric system is not protected, and may be subjected to abuse.
- Genetic tests involve serious privacy issues. In the absence of any strict guidelines, private individuals are misusing it.
- Public and private agencies have increased its modes of surveillance.
- Majority of the respondents agreed that officials of Telecom service providers provide easy access to its subscribers’ personal information.
- Majority of people are totally unaware about their data privacy. They hardly know about how their personal information is being processed by the public and private agencies.

### 12.2 Suggestions

#### 12.2.1 Dealing with Decisional Privacy Rights

It is submitted that the basic instinct of every human being is to grow physically, psychologically, socially, intellectually, and spiritually. For this, the God has blessed us with senses of imagination, exploration, creation, etc. The cumulative effect of all such senses make an individual to take his or her most personal decisions. It reflects that every human being has inherent freedom over their personal autonomy. However, an individual’s instinctive growth gets hampered when his or her personal autonomy is restricted unlawfully or unreasonably.

As the researcher observed, our society has not yet been fully enlightened in accepting the various aspects of an individual’s personal autonomy. Despite the lawfulness of their many personal decisions, individuals face social disapproval whenever they try to execute their personal decisions. Exploratory personal decisions and lifestyles are being severely punished by certain laws and public opinion. Consequently, the individuals apprehend to take their very personal decisions (having no harmful effect over society) regarding their body, marriage, sexual orientation, religious matters, or any other personal matter. Obviously, an individual’s personal autonomous decisions are subject to State’s power. But at the same time the State cannot impose unreasonable restrictions over the individual’s personal decision. It
means that an individual’s reasonable expectation of privacy prohibits the State from interfering with the individual’s personal decisions. Similarly, the State’s positive duty binds its agencies to protect, and help the individuals in executing their personal decisions. But it seems that in our society, the State has failed to protect individuals’ personal autonomy. It seems that in our society, the State is not in a strong position to implement civilized legal principles against the evil practices of social taboos.

Privacy is experienced as ‘room to grow in,’ as freedom from interference, and as freedom to explore, to pursue experimental projects in science, art, work, play, and living.\(^\text{112}\) If exploration and inventiveness in ways to live, play, and interact with others is not permitted or, if permitted, is not conceivable or tolerable to rigidly trained people or is deemed sinful and illegal by the uneducated but trained populace- there is every chance of increasing rates of suicide, alcoholism and drug addiction, and psychological, spiritual, and physical breakdown.\(^\text{113}\)

Therefore, it is suggested that schools and universities must aim at educating more people and at modifying general attitudes toward exploring ways to live. If the general population came to believe (through authentic education and social example) that private life is free, that its privacy is to be respected, and that variety, not uniformity, in ways to live is a value, then the expected catastrophes (like suicide, alcoholism, spiritual breakdown, etc.) may be avoided.\(^\text{114}\)

It is submitted that the true education should be imparted among people, and should have the aim to inculcate the values of respecting each other’s private lives among the members of our society. People’s understanding about one’s private life needs ethical orientation. Exploring ways of today’s lifestyles have to be accepted in our social set up.

It has been argued that those who live exploratory private lives are creating new ways for man to live and be. Therefore, there is an urgent need for changing our present laws and customs so that these explorers-in-private may reveal more publicly the ways in which they have been able to live their lives meaningfully. But without legally guaranteed protection of private life, such experimentation in ways to live and to enrich the experience of leisure life are not likely to be forthcoming.\(^\text{115}\)

Following are some suggestions for protecting ‘decisional privacy’ in our society:

\(^\text{113}\) Id., at 318.
\(^\text{114}\) Ibid
\(^\text{115}\) Ibid
• Education in schools and Universities should inculcate ethical values among people so that general attitude of respecting exploratory ways of one’s private lives is made.

• Through education and government initiated social awareness programs, it is to be ensured that an individual could enjoy his or her ‘freedom of choice’ and other decisional privacy rights meaningfully.

• Since ‘right to marry comes’ within the purview of one’s ‘decisional privacy rights’, it should be protected by the State. But such right becomes meaningless when an individual’s decision to choose the spouse of his or her own choice, is severely criticized and punished by the public opinion. The barbaric practices of ‘honour killings’ have been interfering with the individuals’ private matters of marriage since times immemorial. In order to prevent such incidences, fundamental things are to be done like empowerment of women (physically, socially, psychologically, and financially), stringent domestic violence laws, reformation in administrative and adjudicative processes, collaboration of active police and the government in dealing such offences, impartation of moral and ethical education, making women to realize that they are equal to men, stringent punishments for honour crimes, etc.

• It is the binding duty of the State to make adequate laws for the protection of gays’ and lesbians’ rights. The Constitution of India recognizes and protects the fundamental rights of gays and lesbians. Therefore, the State cannot impose unreasonable restrictions on their fundamental rights of marrying each other. Antiquated laws like sodomy laws having no significance in the liberal society, have to be shunned out from our legal system.

• Similarly, the State should provide a protective atmosphere for the ‘live-in relationship’ couples. This new way of one’s private life in the modern patterns of society should definitely be protected from every public criticism.

• It is suggested that ‘attempt to commit suicide’ should be decriminalized because it aggravates the pain of the accused person. At the same time, one should be allowed to die with human dignity. It is further submitted that ‘dealing with one’s own body’ is again one’s decisional privacy right, therefore, should not be interfered unreasonably and unfairly by the government. Active and passive euthanasia should be allowed in India, but
only after making them subject to strict regulations. Otherwise, it would be
misused in Indian conditions.

12.2.2 Right to Information vis-a-vis Right to Privacy

Not surprisingly, as the researcher observed, Right to Information Act of 2005 have
brought transparency and accountability in the system. Governments collect large amounts of
personal information, and under Right to Information Act any one can demand access to that
information for various reasons. The applicants include investigative journalists, non-
government organizations, civil societies, or any other individual. Although right to privacy
is one of the exemption to one’s freedom to know, the whole mechanism involves many
conflicts. The law relating to Public officials’ right to privacy is not clear in India. The Public
Information Officer (PIO) is the most important functionary in the implementation of the
mechanism (process for application involving third party personal information and privacy
exemption clause) mentioned under Right to Information Act, 2005. In one of the findings,
the researcher came across to know that Public Information Officers (PIOs) lack proper
awareness regarding conflicts between right to privacy and right to information. Obviously,
without knowing the conflicting interests how would they settle such situations. Specifically
in case of public official information, unawareness leads to put public officials’ personal
information at stake. Another problem is of non-applicability of the Right to Information Act
in case of private bodies or individual. In the present digital world where an individual’s
every personal information is being stored in computer databases, our Right to Information
Act is outdated. It needs significant amendments. Following are some suggestions in this
regard:

• For protecting the individuals’ and public officials’ personal information, orientation
  of Public Information Officers (PIOs) must be done by the government agencies so
  that the officers could understand their role, duties and skills.
• It is necessary to define the term ‘personal information’ under Right to Information
  Act. Its interpretation cannot be relied on the common language definitions.
• Privacy exemption requires that every personally identifiable information be
  withheld. But where such information has to be disclosed under certain
  circumstances, data protection principles should be taken into consideration. Both
  the Right to Information and the data protection laws must clearly define how
  personal information is going to be considered.
• It is necessary to define the term ‘public interest’ clearly for settling the conflicting interests i.e. right to privacy and right to information. Moreover, the clear definition of ‘public interest’ is more important to protect the public officials’ right to privacy.

• Both legislations of right to information and right to privacy should be put in a single enactment. In addition, there should be a provision for the appointment of the Privacy Commissioner at centre level and Privacy officers at department level. Privacy commissioners’ and officers’ duties should be fixed. The roles of the privacy commissioner and officer should be of an ombudsman, auditor, consultant, educator, policy adviser, regulator and judge. The Privacy Commissioner should have power to investigate complaints about personal information held by the government, under different legislations. The Privacy Commissioner should also investigate complaints about privacy issues in relation to private sector companies. The functions of the Privacy Commissioner shall be: 116


  b) to conduct an audit of personal information maintained by an agency for ascertaining whether or not the information is maintained according to the information privacy principles. It is suggested that such auditing should be mandatory in nature.

  c) to monitor the use of unique identifiers, and to report the results of that monitoring to some higher authority, including any recommendation relating to the need for, or desirability of taking, legislative, administrative, or other action to give protection, or better protection, to the privacy of the individual.

  d) to examine any proposed legislation that makes provision for the collection of personal information by any public sector agency; or the disclosure of personal information by one public sector agency to any other public sector agency, or both.

  e) to receive and invite representations from members of the public on any matter affecting the privacy of the individual or of any class of individuals.

f) to undertake research into, and to monitor developments in, data processing and computer technology to ensure that any adverse effects of such developments on the privacy of individuals are minimised, and to report to the responsible Minister the results of such research and monitoring.

- The above said functions should be performed by the privacy officers at department level.

- Another function of Privacy Commissioner and Privacy officer is to conduct a privacy impact assessment of proposed rules of the Department on the privacy of personal information, including the type of personal information collected and the number of people affected.  

12.2.3 Role of Media and Right to Privacy

The continuous broadcasting of provocative headlines against the accused persons while the matter is sub-judice has been considered as a violative of the accused person’s right of free trial. Obviously, it is against the basic principles of criminal law. Similarly, the media’s over-inquisitiveness has crossed the levels of decency by showing us the salacious, erotic, or vulgar programs. Idle gossiping over celebrities’ private lives having no public interest involved, reflects media’s irresponsible behaviour towards the society. Nowadays, media’s focus is on the spread of sensationalism. It is orbiting around people’s curiosity to know instead of their ‘necessity to know’. One of the reasons behind sensational media is competitive environment in the concerned field due to commercialization. Therefore, journalists always work under pressure in such exploitive atmosphere. Moreover, these competitive conditions compel newspapers and television news channels to hire unqualified and illiterate journalists having no journalistic sense, and who are totally unaware of professional code of ethics. It has also been observed that investigative journalists lack job satisfaction because of many reasons like unencouraging behaviour of co-journalists, editors, etc. Political biasness of newspapers and Television news channels also discourage a journalist from newsworthy reporting. Therefore, it is necessary to remove such community problems. Moreover, the answer to the problems lies in socio-legal research. Following are some more suggestions for regulating freedom of media:

- It is submitted that the journalists should be made sensitized towards individuals’ privacy rights. They must know how to balance the conflicting interests i.e. right to privacy and freedom of media. They must have the

knowledge about whether their reporting is newsworthy or not. And it is only possible when they are well qualified, and have special communication skills. Therefore, it should be ensured by the government and the media groups that they are taking initiatives for journalistic orientation.

- For investigative journalism, sting operations should be used as a last resort. Primarily, the journalists should be encouraged to opt for alternative means for collecting the same information or news instead of conducting sting operations. Right to Information and similar like legislations should be strengthened and promoted for exposing corrupt practices in the system.

- For ethical journalism, and to avoid prosecution, investigative journalists must also be sensitized towards individuals’ privacy rights. The mere use of hidden cameras and recorders do not replace the journalists’ work of analysing the evidences and reporting a meaningful story.

- Since easily accessible miniature hidden cameras or other sophisticated technological devices are being used in unregulated ways, the strict laws are required to be legislated. Certain self regulatory rules and norms regarding use of such technological devices should also be adopted by the media professionals.

- Sting operations using undercover prostitutes or any other action of inducing a person to commit wrongful act, should be discouraged. For every sting operation, an investigative journalist should take prior approval from some independent, impartial and autonomous body e.g. editorial team of a news channel. The journalist should prove some prima facie facts demanding sting operation, and show the public interest as well as his or her bonafide intentions for conducting sting operation. The journalist shall conduct whole sting operation under the supervision of head of the body.

- Investigative journalism should not be used for gratuitously prying into peoples’ private lives.

- The recordings of a sting operation should be preserved in its original form, and should not be tampered, manipulated, distorted, morphed or otherwise edited in any manner.

- An investigative journalist should have complete details (in writing) of the various stages of progress of a sting operation.
• In case of fabricated sting operations, the concerned persons should be punished strictly.
• The journalists are supposed to know the laws regulating media like defamation, privacy, professional ethics, phone or email tapping, etc. Again, they should focus on their social responsibility i.e. broadcast only those things which are necessary for the informed citizenry.
• Public figures and celebrities’ privacy should be strictly protected in India. By peeping into the public figures’ private lives the journalists may instigate people, direct or indirectly, to spy on each other’s family life or individual life.
• A privacy ombudsman should be appointed to investigate the complaints of privacy violations committed by media professionals. The ombudsman should have power to adjudicate the matter suo moto, and to remedy the victims with adequate compensation. Again, it is necessary that whole process should be speedy and less expensive one. Moreover, the privacy ombudsman’s order should have binding authority.
• In India, it has been observed that freedom of media is broadly regulated by the self regulatory mechanism. But the present self regulatory mechanism has failed in its responsibility to regulate ‘freedom of press’ in India. Similarly, recent incidences of sensational and over-inquisitive media (where innocent private lives were intruded) is demanding strict laws for regulating media in India. Moreover, in a very recent judgment the Delhi High Court was hearing a Public Interest Litigation against a reality show ‘Emotional Atyachar’ telecast on United Television (UTV) Bindass alleging the use of indecent, obscene and vulgar language in the programme which was offending good taste and decency as well as being offensive to the sensibilities of children. While discussing the advantages and disadvantages of self-regulation, a Division Bench constituting Justice Pradeep Nandarajog and Justice Pratibha Rani rejected the idea of self-regulation of the broadcasters and highlighted the necessity of state intervention in the regulation of electronic media. The Delhi High Court recommended that a statutory regulatory body be constituted consisting of men and women of eminence, for
regulating electronic media in India. But at the same time, the freedom of speech and expression cannot be restricted unreasonably. Therefore, the researcher views to find out some mid path. It is submitted that Justice Leveson Inquiry Report should be adopted in India. The brief recommendations of the report are as follows:

a) An independent regulatory body for the press should be established.
b) The body should have the power to investigate serious breaches and sanction newspapers.
c) It is essential that there should be legislation to underpin the independent self-regulatory system and facilitate its recognition in legal processes. It means that a new legislation is required to have check over the new self regulatory body.
d) An arbitration system, as an alternative to the courts of law, should be created for redressing the victims’ grievances.
e) If a newspaper publisher who chose not to subscribe to the regulatory body was found to have infringed the civil law rights of a claimant, it could be considered to have shown wilful disregard of standards and thereby potentially lead to a claim for exemplary damages. Newspapers that refuse to join the new body could face direct regulation by media watchdog Ofcom. The Office of Communications commonly known as Ofcom, is the government-approved regulatory and competition authority for the broadcasting, telecommunications and postal industries of the United Kingdom. It has been recognized under the Office of Communications Act of 2003.
f) New regulatory body includes the establishment of an independent appointments panel which could include one current editor but with a substantial majority demonstrably independent of the press. The board and chair of such a body should all be appointed by a fair and open process, comprise a majority that are independent of the press, include

---

118 Indraprastha People v. Union Of India, decided on 9 April, 2013, in the High Court of Delhi, WP(C)No.1200/2011. Available at http://indiankanoon.org/doc/80393956/ accessed on August 20, 2013, at 3:00 p.m. IST.

a sufficient number of people with experience of the industry who may include former editors and senior or academic journalists, but shall not include any serving editor or member of the House of Commons or government. It is also recommended that a ‘code committee’ should be created in which serving editors have an important part to play although not one that is decisive. This committee would then advise the new body. There is also a proposal to include purely voluntary pre-publication advice service to editors.

g) Leveson also recommends the establishment of a whistle-blowing hotline for journalists, and says the new body should encourage its members to ensure that journalists’ contracts include a conscience clause protecting them.

In addition to above, it is submitted that right to privacy should be incorporated in the Constitution of India, and should be made a ground of reasonable restrictions on the freedom of speech and expression.

12.2.4 Children’s Online Privacy

In one of the findings, the researcher found that the Children, in general, are using online services without any sense of responsibility. Due to lack of parental control and guidance, the children have got very easy accesses to the internet services. Obviously, it has many serious implications. An ignorant child may get indulged in cyber crimes including violation of an individual’s privacy rights. At the same time, he or she could be victimized by online abusers. Thus, adequate legislations are required to protect children’s online privacy. Indeed, the Delhi High Court in 2013 asked Google Inc and Facebook Inc about the mechanism to deal with a misuse of social networking sites by children below 13 years of age. The bench of the Delhi High Court showed its concern over the issue of minors’ accounts at social media networking sites, and frowned on the fact that they are also being lured into illegal activities, either knowingly or unknowingly. According to reports the court’s direction came after counsel for Facebook submitted that the site operated under the United States law Children’s Online Privacy Protection Act (COPPA) as per which a child below 13 is not allowed to open an account. The Court expressed unhappiness that there is no mechanism that currently exists to verify the age of a child online, and that while children
were protected in the United States, what of the children in India. The court also remarked that India is behind time on online protection of children.

The United States’ law of Children’s Online Protection Act of 1998 specifically protects the privacy of children under the age of 13 by requesting parental consent for the collection or use of any personal information of the users. The Act took effect in April 2000. The Act was passed in response to a growing awareness of Internet marketing techniques that targeted children and collected their personal information from websites without any parental notification. The Act applies to commercial websites and online services that are directed at children.

Following are the main requirements of the Children’s Online Protection Act of 1998:

- It is mandatory for the website and online service operators to display privacy policy about the collection, uses, and disclosure of personal information of children.
- The website operators have to obtain verifiable parental consent for the collection, use, or disclosure of personal information from children. Verifiable parental consent means any reasonable effort (taking into consideration available technology) including a request to parents for the authorization for future collection, use and disclosure of child’s personal information. Moreover, it should be disclosed to parents of any information collected on their children by the website.
- Acquisition of a verifiable parental consent prior to collection of personal information from a child under the age of 13.
- A Right to revoke consent and have information deleted.
- Where a child plays online games, there should be a limited collection of personal information.
- It is mandatory for the operators to protect the confidentiality, security, and integrity of children’s every personal information (which is collected online).

120 Mahima Kaul, “Indian court orders Facebook, Google to offer plans for protecting children,” available at http://www.indexoncensorship.org/2013/08/indian-court-orders-facebook-google-to-offer-plans-for-protecting-children/ accessed on August 20, 2013, at 3:00 p.m. IST.
121 “India behind time on online protection of children: Delhi High Court,” The Economic Times, July 16, 2013. Available at http://articles.economictimes.indiatimes.com/2013-07-16/news/40613307_1_social-networking-sites-web-sites-veerag-gupta accessed on August 20, 2013, at 3:00 p.m. IST.
122 “Children’s Online Privacy Protection Act (COPPA),” available at http://epic.org/privacy/kids/ accessed on August 20, 2013, at 3:00 p.m. IST.
The Federal Trade Commission adopted final amendments to the Children’s Online Privacy Protection Rule that strengthens kids’ privacy protections and gives parents greater control over the personal information that websites and online services may collect from children under 13. The Federal Trade Commission initiated a review in 2010 to ensure that the Children’s Online Privacy Protection Rule keeps up with evolving technology and changes in the way children use and access the Internet, including the increased use of mobile devices and social networking. The updates to the Children’s Online Privacy Protection Rule reflect careful consideration of the entire record of the rulemaking, which included a public roundtable and several rounds of public comments sought by the agency.123

The final amendments in Children’s Online Privacy Protection Rule are as follows:

- ‘Personal Information’ that cannot be collected without parental notice and consent, also includes geolocation information, photographs, videos, and child’s image and voice.
- Even third parties cannot collect personal information from children through plug-ins without parental notice and consent.
- Children’s Online Privacy Protection Rule covers persistent identifiers that can recognize users over time and across different websites or online services, such as Internet Protocol IP addresses and mobile device IDs.
- The rules require website operators to adopt reasonable procedures for data retention and deletion.
- The rules also strengthen the Federal Trade Commission’s oversight of self-regulatory safe harbor programs.
- The amendments add several new methods that operators can use to obtain verifiable parental consent: electronic scans of signed parental consent forms; video-conferencing; use of government-issued identification; and alternative payment systems, such as debit cards and electronic payment systems, provided they meet certain criteria.124

Therefore, it is submitted that the website operators should legally be compelled to adopt such technological ways through which parents’ informed consent be taken as well as child’s actual physical age be identified online. Increasingly, it is also necessary on the part of the

123 “FTC Strengthens Kids’ Privacy, Gives Parents Greater Control Over Their Information By Amending Children’s Online Privacy Protection Rule,” available at http://www.ftc.gov/opa/2012/12/coppa.shtm accessed on August 20, 2013, at 3:00 p.m. IST.
124 Ibid.
government as well as website operators to take strong initiatives for educating parents (so that they could have proper check over their minor children’s online activities).

12.2.5 Need for Regulating Social Networking Sites in India

It is submitted that people are nowadays getting fascinated with the concept of online social media. They use to share information and communicate with their friends and strangers on the social networking sites (e.g., Facebook, MySpace, Friendster, Orkut, etc.). As the researcher found in the survey, the users do care for their privacy settings at social networking sites. They do not want to share all of their information with everyone. However, many of the users are not satisfied with the privacy settings of the social networking sites. Moreover, in many cases the users struggle to customize their privacy settings because they feel that the ‘privacy settings’ are so complex and time consuming. In addition to this, many users are illiterate and totally unaware of any privacy settings. Therefore, their unawareness also subject them to cyber stalking, cyber bullying, morphing, etc. Thus, it is necessary to bring new social media policies in India. While adopting any policy in India, it is submitted that following recommendations should be considered:

- A child, who is less than thirteen years of age, should not be allowed to make an account on these social networking sites. In addition, the social networking sites should have some technology (may be in the form of some software or physical device or anything solving the purpose) through which the age of the user be identified.
- Social networking sites should make the privacy settings an easy process. The sites should upload some software on their webpage whose goal is to automatically configure a user’s privacy settings using only a small amount of effort from the user.\(^{125}\)
- Privacy policies, like all agreements, should be clear and easy to follow, so that users have a firm grasp on what they are signing-up to.\(^{126}\)
- It is submitted that the government as well as the social networking sites should take initiatives for spreading awareness among the illiterate and unaware users.
- There is need to strengthen the cyber police system in India. An online reporting system is required where online users could complaint against cyber crimes.

---


\(^{126}\) “Social Networking Sites,” available at http://epic.org/privacy/socialnet/ accessed on August 20, 2013, at 3:00 p.m. IST.
cyber police may also prevent cyber crimes by informing parents, students, schools, etc. about the issue. The users should be encouraged for reporting the cyber crime. Where the online abuser’s server is situated outside India, the cyber police should be attached globally with foreign states’ cyber units so that they would access the abusers’ online information.

- Facebook’s ‘Tag Suggest’ feature currently identifies faces in newly uploaded photos by comparing them with pictures in which the users have previously been tagged. Facial recognition software is used to calculate a unique ‘template’ based on someone’s facial features, like the distance between the eyes, nose and ears. By using a mixture of information about facial shape and features, and contextual clues such as other people in the same album or picture, Facebook is able to suggest to users the names of other people in photos they have taken. Facebook implemented the Tag Suggest feature as an automatic opt-in for all users. That, combined with the fact that most photos on Facebook aren’t uploaded by their subjects—obviously, since someone is normally behind the camera—meant that it necessarily played fast and loose with privacy concerns. The Irish Data Protection Commissioner in 2012 ruled that Facebook must be opt-in to comply with local privacy laws. The Data Protection Commissioner also required Facebook to provide a prominent warning to its European users that it uses facial recognition technology that automatically tags them in photographs. The social network was then forced to switch off its facial recognition tool and delete data collected from European users in October 2012, following an investigation by privacy authorities in Ireland and Germany. Therefore, it is submitted that the social networking sites should be prohibited to launch such invasive applications in India. At least, some authority should be established to regulate social networking sites’ functioning in India. By doing this, it would be possible for the authority to audit and review the new applications and privacy settings of the social networking sites.

---

127 By Sophie Curtis, “Facebook may use profile pictures for facial recognition,” The Telegraph 10:38 A.M BST 30 Aug 2013, available at [http://www.telegraph.co.uk/technology/facebook/10275564/Facebook-may-use-profile-pictures-for-facial-recognition.html](http://www.telegraph.co.uk/technology/facebook/10275564/Facebook-may-use-profile-pictures-for-facial-recognition.html) accessed on August 20, 2013, at 3:00 p.m. IST.


129 By Sophie Curtis, “Facebook may use profile pictures for facial recognition,” The Telegraph 10:38 A.M BST 30 Aug 2013, available at [http://www.telegraph.co.uk/technology/facebook/10275564/Facebook-may-use-profile-pictures-for-facial-recognition.html](http://www.telegraph.co.uk/technology/facebook/10275564/Facebook-may-use-profile-pictures-for-facial-recognition.html) accessed on August 20, 2013, at 3:00 p.m. IST.
• It is submitted that Section 66A\textsuperscript{130} of the Information Technology Act is being misused against the political dissenters. Therefore, it becomes necessary on the part of the government to introduce more privacy parameters in such kind of provisions. Otherwise, it amounts to violation of one’s right to speak freely, freedom to speak anonymously, and freedom of association. Cumulatively, all these rights are the parts of individual’s privacy rights.

• In the latest Google Transparency Report of 2012, it was admitted that Google regularly receives requests from government agencies and courts around the world to remove content from its services. Governments ask companies including Google and other technology and communication companies, to remove content for different reasons like, allegations of defamation, the content violates local laws prohibiting hate speech or adult content, etc.\textsuperscript{131} Jeffrey Rosen calls officials at Internet and telecom companies like Google, Facebook, Twitter, Verizon, and AT&T, the deciders. He argues that the officials and telecom companies the ones who decide what controversial speech stays up and what comes down in response to government demands or users’ objections. Therefore, whoever controls the information databases holds the real power to decide who can speak and what we can say.\textsuperscript{132} It is submitted that Social Networking Sites are bound to protect its users’ human rights. The sites should not provide easy access to anyone unless there is some probable cause. The sites should make strict policies in this regard.

\textsuperscript{130} The Information Technology Act, 2000, s. 66A.

Punishment for sending offensive messages through communication service, etc.,

Any person who sends, by means of a computer resource or a communication device,—

(a) any information that is grossly offensive or has menacing character;
(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently by making use of such computer resource or a communication device,
(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages shall be punishable with imprisonment for a term which may extend to three years and with fine.

Explanation: For the purposes of this section, terms “electronic mail” and “electronic mail message” means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, images, audio, video and any other electronic record, which may be transmitted with the message.

\textsuperscript{131} “Google Transparency Report,” available at http://www.google.com/transparencyreport/removals/government/ accessed on April 9, 2013, at 5:00 p.m. IST.

Snowden’s disclosure about United States’ spying has alarmed the Indian government to think over its use of social media sites. For example, Prime Minister Office itself uses gmail for communications. The researcher argues that the Indian government should investigate the whole United States’ spying matrix for protecting its citizens’ privacy. The government should take strong actions similar to that of European Union and Commission actions on the United States’ surveillance.

However, the Supreme Court of India refused to entertain a Public Interest Litigation seeking direction to the government to initiate action against internet companies involved in sharing internet data from India with United States National Security Agency. The apex court said it cannot entertain the petition as Indian agency is not involved in it and allowed the petitioner, former dean of law faculty of Delhi University S N Singh, to move any other forum for seeking remedy against internet companies and the United States agency for snooping data resulting in violation of right to privacy. In his plea, Singh alleged that such large scale spying by the United States authorities is detrimental to national security and urged the apex court to intervene in the matter. He claimed internet companies were sharing information with the foreign authority in breach of contract and violation of right to privacy.

At the same time, it is apt to mention that the European Parliament has voted overwhelmingly (483 to 98, with 65 abstentions) to investigate ‘PRISM’ and other surveillance programs of the United States National Security Agency. The investigation with be undertaken by the influential Committee on Civil Liberties, Justice, and Home Affairs (‘LIBE’). Members of Parliament also urged European representatives to re-examine current arrangements that allow the transfer of banking and travel data from European Union countries to the United States. The resolution was adopted as the European Union is considering a new trade deal with the United States and a proposal to strengthen privacy protections is pending. Similarly, European Justice Commissioner Viviane Reding has asked United States’ Attorney General Eric Holder to explain the scope of United States data collection about European Union (EU) citizens. 

---

133 “How NSA hacks the whole world,” http://www.frontline.in/cover-story/how-nsa-hacks-the-whole-world/article4849218.ece accessed on August 29, 2013, at 11:00 a.m. IST.
135 “European Parliament to Investigate US NSA Surveillance Programs and impact on EU Citizens’ Privacy,” Electronic Privacy Information Center, July 5, 2013. Available at http://epic.org/privacy/intl/eu_data_protection_directive.html accessed on August 30, 2013, at 1:00 p.m. IST.
Alternatives of Excessive Surveillance Techniques need to be explored

Analyzing the primary and secondary data, the researcher observed that excessive surveillance involves serious physical and psychological implications. The excessive use of surveillance techniques, both by public and private bodies, has increased the probability of violation of an individual’s privacy rights including freedom of speech and expression, freedom of movement, freedom of association, freedom of religion, personal autonomy, right to life and personal liberty, etc. Substantial number of respondents in the survey, which was conducted by the researcher in Chandigarh, has the view that the present surveillance system is not successful in reducing the crimes. Therefore, it is submitted that the focus should be on the effectiveness of the surveillance system. The surveillance techniques should be made successful to reduce crimes. At the same time, the surveillance techniques should be less intrusive into private lives. The surveillance methods should be benefitting the society and accepted by the public at large.

Furthermore, it is submitted that the people cooperate in providing their information to the government because they do believe in the government’s mode of collection of individuals’ personal information, e.g. in census survey, department forms, aadhar forms, permanent account number forms, bank forms, etc. People expect that the government and its agents work efficiently in protecting the individuals’ personal information. It means that the government is expected to maintain a balance between state’s security and individual’s privacy. It is people’s cooperation and trust which empower the government to make policies, laws, and regulations for the whole society. Obviously, distrustful government would not be able to run the democratic set up efficiently. Therefore, it is submitted that the government should protect individuals’ right to privacy; otherwise it would result into people’s distrust in the government. For this, the government should avoid the methods of excessive surveillance unless it has strong justification. Again, an individual should be provided with more rights of challenging the government’s surveillance actions including the actions’ scrutiny by privacy ombudsman.

The researcher also observed in the research that the governments and other organizations are indulged in the practice of using surveillance tools for the political purposes. In order to prevent their criticism, the governments and organizations keep surveillance over the political dissidents.

Roger Clarke argues that men in power do not want innovations, change, or dissidence. It is so because of the fact that they are threatened by change, and believe that risks need to be suppressed rather than managed. Sustaining progress is possible by
protecting people’s being and feeling, freedom to propose, discuss, articulate and publish new ideas. A cluster of freedoms relating to human identities is fundamental to cultural, economic and political innovation: the freedom to have and to use multiple identities, the freedom to express ideas by means of pseudonyms, and the freedom to avoid linkage among identities.136

It is apt to mention about the Edgar Hoover’s (First Director of the Federal Bureau of Investigation) modes of surveillance. It has been stated that he used to blackmail the political dissenters by intercepting their communications.137 Harry S Truman wrote during his presidency, “We want no Gestapo or secret police. Federal Bureau of Investigation (FBI) is tending in that direction. They are dabbling in sex-life scandals and plain blackmail… Edgar Hoover would give his right eye to take over, and all congressmen and senators are afraid of him.” Moreover, for half a century, the Federal Bureau of Investigation (FBI) director waged war on homosexuals, black people and communists.138

Increasingly, what would happen if the government starts prosecuting and convicting dissenters for posting content online? This frightening story is of Shi Tao. In 2005, he composed an email from his office in China using a Yahoo account, which he then sent to a pro-democracy website in New York City. He attached to the email an article, which he wished to publish anonymously, on China’s new policies regarding crackdowns on potential pro-democracy dissidents in China. When Chinese authorities became aware of the article they considered it a breach of state secrets and sought to find out the author. They eventually received crucial information about Shi Tao’s identity from Yahoo’s Asian business partners in Hong Kong. This evidence was then used to convict him in a Chinese court.139

Therefore, it is submitted that surveillance tools should not be used for taking revenge from the opponents or dissidents. Surveillance should be made accountable at all public or private places. The subjects should know that they are being watched. For example, the subjects should be made aware about the exact location of cameras, and should have the access to the camera images or recordings.

It means that the individuals need to know when their treatment is due to profiling, so that they can dispute the profiling and the treatment. They need to be clear on who is accountable for protection of their data, and how they are protected if their data are used fraudulently. Generally, they need to have a clear role in reciprocal relationships between themselves and the state or the companies they deal with. Finally, individuals need to be aware of their rights and responsibilities when it comes to the processing of their personal data. Education is key to enabling people to protect themselves against fraud, stand up for themselves in the face of profiling, and protect data that they can and wish to keep private. Alongside education there needs to be ease of access to the processes that allow people to protect themselves.

Increasingly, it is essential that failure modes should be fully explored before the implementation of technology such as biometric identity cards, in order to foresee the problems which might arise, and how they can be dealt with. Moreover, the public as well as private sector should also adopt the mechanism of installing privacy enhancing technologies, and framing privacy impact assessment. For example, the public and private agencies should adopt some privacy friendly technologies to replace indecent practices of frisking and pat down searches. Jeffrey Rosen, Professor at George Washington University, advocates ‘blob machine’ as an alternative to full body scanners. The naked machines reveal not only contraband, metal, or plastics concealed under clothing, but also graphic images of the naked body. There is also an apprehension of stored or recorded images being abused. Hence, naked machine threatens individuals’ privacy. Whereas, in case of ‘blob machines’, only the area of suspicion is revealed, and the screen shows rest of the body as blob-like human image. It is also seen that both types of machines offer identical amounts of security. Therefore, for the sake of privacy protection, public and private agencies should adopt ‘blob machines’ which really preserve privacy.

It is submitted that blob machines should be installed as an alternative to frisking at every place like Airport, a shopping mall, a multiplex, etc. It will really spread a sense of

141 Ibid.
142 Id., at 45.
dignified life among people who would be subjected to frisking. Only blob machines can bring the balance between privacy and security.

It is further submitted that the State should appoint a Privacy Ombudsman and Privacy Commissioner for redressing the privacy issues.

12.2.7 Biometric System Should Be Made Privacy Friendly

Biometric information is part of an individual’s identity, and a loss of control over that information can threaten autonomy and liberty. Human recognition systems are inherently probabilistic, and hence inherently fallible. The chance of error can be made small but not eliminated. System designers and operators should anticipate and plan for the occurrence of errors, even if errors are expected to be infrequent. The scientific basis of biometrics—from understanding the distributions of biometric traits within given populations to how humans interact with biometric systems—needs strengthening particularly as biometric technologies and systems are deployed in systems of national importance. Biometric systems should be designed and evaluated relative to their specific intended purposes and contexts rather than generically. Their effectiveness depends as much on the social context as it does on the underlying technology, operational environment, systems engineering, and testing regimes.

According to Roger Clarke, Biometric technologies don’t just involve collection of information about the person, but rather information of the person, intrinsic to them. That alone makes the very idea of these technologies distasteful to people in many cultures, and of many religious persuasions. In addition, each person has to submit to examination, in some cases in a manner that many people regard as demeaning. Biometrics system may involve following privacy threats:

a) Privacy of Personal Behaviour

Biometric monitoring of people’s movements and actions increases the transparency of individuals’ behaviour to organizations, and brings the organizations at perfect position to anticipate actions that they would prefer to prevent. Moreover, an organization may share one’s biometric information

---

144 Joseph N. Pato and Lynette I. Millett (Eds.), Biometric Recognition: Challenges and Opportunities, 100 (2010).
145 Id., at 1.
146 Id., at 2.
147 Ibid.
with other organisations, such as business partners, corporations and
government’s agencies.

b) Denial of Anonymity and Pseudonymity

Biometric technologies have the potential to deny any kind of anonymity in
coming future.

c) Masquerade

It is believed that the stored biometric information may be fabricated to make
replicas of a particular person.

d) Permanent Identity-Theft

Organizations may be misled during its transactions because of person’s
identity theft.

e) Automated Denial of Identity

Identity theft is not limited to individual criminals. For example, a corporation
could apply biometrics to the denial of access to premises by ex-employees,
customers previously found guilty of shop-lifting, and in the case of casinos,
problem-gamblers.

f) Dehumanisation

Many believe such practice as a dehumanizing one. A Biometricized
individual may be considered as a commodity or a thing, which is against the
principles of ethics.

Roger Clarke suggested certain safeguards which are as follows:149

- Self-Regulation: It is one of the possibility which can be relied
  upon. However, Clarke believes that Biometrics providers are eager suppliers
to repressive governments in the third world.
- Compulsory Social Impact Assessments: The process requires
  that full public disclosure of the technologies and the applications that are
  envisaged; appropriately-funded social impact analysis; publication and
  consultation; active public participation in scheme design; and controls built
  into the scheme.
- Generic Privacy Laws: Biometric technologies might be
  precluded or regulated by existing privacy protection laws including ‘fair
  information practices’.

149 Ibid.
• Specific Regulation: Specific legislations are required on the topic. In addition, technological solutions should adopted like the production of a tool for masquerade is not possible; design standards for biometric measuring devices, such that they can be shown to not permit the biometric to be accessed or captured; prohibition of the manufacture or import of biometric measuring devices that do not comply with the design standards; the installation and use of biometric measuring devices that do not comply with the design standards; etc.

It is submitted that privacy enhancing technologies should be installed in the present Biometric system in India.

The one-off use of fingerprints in medical screening is a biometric application that enhances privacy. This makes having to use patient names to match with their diagnostic results unnecessary. There is a double advantage to the one off use of biometrics in this instance: patients can remain anonymous and there is greater reassurance that data are released to the correct person. Another obvious example is the ex post measure already mentioned biometric authentication to restrict operator use in a database. This use of biometrics makes operators more accountable for any use/misuse of data. A more generic example is the match on card-sensor on card: biometric authentication without the biometric characteristics leaving devices owned by the individual. Biometric cryptography is a privacy enhancing technical solution that integrates an individual’s biometric characteristics in a revocable or non-revocable cryptographic key.  

12.2.8 Radio Frequency Identification (RFID)

RFID is a method for exchanging information between a marker (radio tag), which can be incorporated into any object, and a reader, a wireless device that identifies the information using radiofrequencies. The technology is more powerful when the reader is linked to communication networks such as the internet, which makes the information available over the world-wide web.


The widespread deployment of Radio frequency technology has brought significant changes in the development of many sectors, including transport, health and retail trade. Its applications range from the traceability of food, to automated payments, and the mobility and observation of patients suffering from Alzheimer's disease. Therefore, it also improves people’s lives. However, the technology has raised many confidentiality issues and security concerns as it can be used to gather and distribute personal data. Consequently, it would be difficult to get public acceptance for such technology. Therefore, it is necessary to figure out the social, political, ethical and legal implications of the technology before its deployment.\textsuperscript{152}

In addition, it is necessary to focus on each individual Radio frequency device (RFID) application since each application has its own risks and advantages. Moreover, awareness and information campaigns for poorly informed people should be initiated to inform them about the challenges of the Radio Frequency (RFID) technology. The European Union protects personal data under Article 8 of the Charter of Fundamental Rights, general Data Protection Directive and the ePrivacy Directive. These Directives guarantee the protection of personal data, while taking account of innovations in data processing procedures.\textsuperscript{153}

European Commission has given some recommendations for dealing with Radio Frequency Identification technology, which are as follows:\textsuperscript{154}

- Member States should ensure that industry, in collaboration with relevant civil society stakeholders, develops a framework for privacy and data protection impact assessments.
- Member States should ensure that operators conduct an assessment of the implications of the technology for the protection of personal data and privacy, including whether the application could be used to monitor an individual. It means that the operators should decipher the privacy risks which are involved in the implementation of the technology. Moreover, a person or group of persons should be designated to review the privacy impact assessments.
- Member States should support the Commission in identifying those applications that might raise information security threats with implications for the general public. For such applications, Member States should ensure that operators, together with national

\textsuperscript{152} Ibid.
\textsuperscript{153} Ibid.

704
competent authorities and civil society organisations, develop new schemes, or apply existing schemes, such as certification or operator self-assessment, in order to demonstrate that an appropriate level of information security and protection of privacy is established in relation to the assessed risks.

- Member States should ensure that operators develop and publish a concise, accurate and easily understandable information policy for each of their applications. The policy should at least include the complete address of the operators, the purpose of the application, identification of the personal data (which is to be processed), and whether the location of tags will be monitored, data protection impact assessment, privacy risks (if any) relating to the use of tags in the application and the measures that individuals can take to mitigate these risks.

- Consumers should be informed of the presence of radio frequency (RFID) tags placed on or embedded in products, and that tags should be removed or deactivated immediately-and without a fee-at the point of sale, unless a purchaser expressly consents to keep a tag operational. The operator should notify the privacy impact assessment of the radio tags.

- Member States, in collaboration with industry, the Commission and other stakeholders, should take initiatives to inform and raise awareness among public authorities and companies of the potential benefits and risks associated with the use of RFID technology. Specific attention should be given to information security and privacy aspects.

- Member States, in collaboration with industry, civil society associations, the Commission and other relevant stakeholders, should identify and provide examples of good practice in the implementation of radio frequency (RFID) applications to inform and raise awareness among the general public.

Therefore, it is submitted that such recommendations should be adopted in India before implementing the radio frequency applications in every sphere of the society. In India, there is an urgent need to inform and raise awareness level among general public about the issues, challenges, and good practices of the radio frequency technology.

It is submitted that radio frequency devices attached with Global Positioning systems should not be used by the law enforcement agencies to track the suspects, offenders, etc. Such action would be a dehumanizing one, and involves both physical and psychological implications.
12.2.9 Deoxyribonucleic acid (DNA) Profiling and Privacy Issues

The collection and use of Deoxyribonucleic acid (DNA) for criminal justice involves following privacy issues:

- It has increased governmental physical and psychological intrusion has been increased.

- Deoxyribonucleic acid (DNA) searches may be conducted by the law enforcement agencies even without taking any consent of the individual. Moreover, the courts are of the view that an individual has no reasonable expectation of privacy in case of abandoned Deoxyribonucleic acid (DNA) e.g. where Police extracts suspects’ Deoxyribonucleic acid (DNA) using articles such as cigarette butts or envelopes, cold drink bottles or cans.

- The genetic similarity of close relatives allows the use of Deoxyribonucleic acid (DNA) of one family member to suggest whether another family member has committed a crime. Police thus may follow a close relative in the hopes of collecting a discarded tissue or coffee cup and use the Deoxyribonucleic acid (DNA) on that object to compare to a Deoxyribonucleic acid (DNA) profile obtained at the crime scene.\[^{155}\]

- The government’s retention of the biological sample from which the Deoxyribonucleic acid (DNA) profile was derived also raises privacy concerns. While the Deoxyribonucleic acid (DNA) profile may not code for particular traits, the genetic sample contains intensely personal information about genetic disorders, familial relationships, and, in the future, perhaps predilection to certain behavioral traits such as a propensity to antisocial behavior. As long as the samples are stored, there exists a possibility that the state (or an unauthorized third party) may access and then misuse this kind of information—whether by disclosing it for retributive reasons, by detaining those predisposed to antisocial behavior to serve crime control purposes, or simply accidentally releasing the information.\[^{156}\]

---


156 Ibid.
It is also believed that the use and expansion of law enforcement DNA
databases may deepen the racial inequalities in the criminal justice system and
exacerbate minorities’ distrust of law enforcement.\textsuperscript{157}

In \textit{Maryland v. King},\textsuperscript{158} the United States Supreme Court held that when officers make an
arrest supported by probable cause to hold for a serious offense and they bring the suspect to
the station to be detained in custody, taking and analyzing a cheek swab of the arrestee’s
Deoxyribonucleic acid (DNA) is, like fingerprinting and photographing, a legitimate police
booking procedure that is reasonable under the Fourth Amendment.\textsuperscript{159}

However, Justice Scalia along with Justice Ginsburg, Justice Sotomayor, and Justice
Kagan gave the dissenting opinion in this case. He strongly criticized the majority decision.
Although Justice Scalia acknowledged the capability of the Deoxyribonucleic acid (DNA)
testing to solve crimes, the prime responsibility of the Constitution is to protect people from
suspicionless law-enforcement searches. He argued that every suspicionless search requires
non-investigative motive. He wrote:

\begin{quote}

Today’s judgment will, to be sure, have the beneficial effect of solving
more crimes; then again, so would the taking of DNA samples from
anyone who flies on an airplane (surely the Transportation Security
Administration needs to know the “identity” of the flying public),
applies for a driver’s license, or attends a public school. Perhaps the
construction of such a genetic panopticon is wise. But I doubt that the
proud men who wrote the charter of our liberties would have been so
eager to open their mouths for royal inspection.\textsuperscript{160}
\end{quote}

Scalia says that Deoxyribonucleic acid (DNA) testing takes weeks to process, and police
almost always get the results long after they’ve confirmed the identity of people they’ve
arrested. He wrote

\begin{quote}

[T]he court’s assertion that DNA is being taken, not to solve crimes, but
to identify those in the state's custody taxes the credulity of the
credulous.\textsuperscript{161}
\end{quote}

Winfree said that since 2009, when it began testing the Deoxyribonucleic acid (DNA) of
people arrested for violent crimes, Maryland had obtained 225 matches, 75 prosecutions and

\begin{footnotesize}
\begin{enumerate}
\item \textit{Ibid.}
\item Decided On June 3, 2013, 12-207 (2013). Available at http://supreme.justia.com/cases/federal/us/569/12-207/opinion3.html accessed on July 12, 2013, at 2:00 p.m. IST.
\item \textit{Id.}, at 28.
\item Scalia, J., dissenting, \textit{Id.}, at 18.
\item \textit{Id.}, at 1.
\end{enumerate}
\end{footnotesize}
42 convictions. Scalia responded, “Well, that’s really good. I’ll bet you if you conducted a lot of unreasonable searches and seizures, you’d get more convictions, too. That proves absolutely nothing.” In light of the enormous amount of personal information that can be gleaned from Deoxyribonucleic acid (DNA), Justice Sotomayor noted that there is something inherently dangerous about DNA collection that is not the same as fingerprinting. After seizing Deoxyribonucleic acid (DNA) on arrest, for example, the government might choose to profile a suspect’s entire genome more broadly, looking for a predisposition to violence, for example, that could be used to deny people bail or even health insurance.

In India, section 53 of the Criminal Code of Procedure allows medical practitioners, only after police officer’s authorization, to examine a person arrested on the charge of committing an offence and with reasonable grounds that an examination of the individual will bring to light evidence regarding the offence. This can include the examination of blood, blood stains, semen, swabs in case of sexual offences, sputum and sweat, hair samples, and finger nail clippings, by the use of modern and scientific techniques including Deoxyribonucleic acid (DNA) profiling and such other tests which the registered medical practitioner thinks necessary in a particular case.

However, the above said provision is silent about the mechanism for handling the collected Deoxyribonucleic acid (DNA) evidences. The provision also fails to explain that

---


It provides:
53. Examination of accused by medical practitioner at the request of police officer.
(1) When a person is arrested on a charge of committing an offence of such a nature and alleged to have been committed under such circumstances that there are reasonable grounds for believing that an examination of his person will afford evidence as to the commission of an offence, it shall be lawful for a registered medical practitioner, acting, at the request of a police officer not below the rank of sub-inspector, and for any person acting in good faith in his aid and under his direction, to make such all examination of the person arrested as is reasonably necessary in order to ascertain the facts which may afford such evidence, and to use such force as is reasonably necessary for that purpose.
(2) Whenever the person of a female is to be examined under this section, the examination shall be made only by, or under the supervision of, a female registered medical practitioner.

Explanation.--In this section and in sections 53A and 54,-
(a) “examination” shall include the examination of blood, blood stains, semen, swabs in case of sexual offences, sputum and sweat, hair samples and finger nail clippings by the use of modern and scientific techniques including DNA profiling and such other tests which the registered medical practitioner thinks necessary in a particular case;
(b) “registered medical practitioner” means a medical practitioner who possess any medical qualification as defined in clause (h) of section 2 of the Indian Medical Council Act, 1956 and whose name has been entered in a State Medical Register.
what will happen to the evidence after it is collected and analysed. Again, it is unclear whether the Deoxyribonucleic acid (DNA) specimens will be retained for future searches or not. Therefore, it is necessary to make a comprehensive legislation to regulate the collection, use, analysis and storage of Deoxyribonucleic acid (DNA) samples, including for crime-related purposes in India.

Recognizing the need to create an appropriate legislation to regulate various issues relating to Deoxyribonucleic acid (DNA) profiling and establishment of Deoxyribonucleic acid (DNA) data banks, quality control, obligations and accreditation of Deoxyribonucleic acid (DNA) laboratories, the Department of Biotechnology (DBT) set up a Deoxyribonucleic acid (DNA) Profiling Advisory Committee (D-PAC) in December 2003 to make recommendations for enacting a suitable legislation. The D-PAC comprising experts from the relevant fields submitted its report and a draft Human DNA Profiling Bill in 2006. One of the important provisions of the Bill is the establishment of Deoxyribonucleic acid (DNA) data banks, that would help the criminal justice system in solving cases and also in crime prevention. It is known that a number of crimes are committed by repeat offenders, who could be apprehended and convicted by comparison of evidence at the scene of crime with information a Deoxyribonucleic acid (DNA) data bank.165

However, the Parliament did not introduce Human Deoxyribonucleic acid (DNA) Profiling Bill. In February 2012, a new version of the Bill was leaked. If passed, the Bill will establish state-level Deoxyribonucleic acid (DNA) databases which will feed into a national-level Deoxyribonucleic acid (DNA) database, and proposes to regulate the use of Deoxyribonucleic acid (DNA) for the purposes of enhancing protection of people in the society and the administration of justice.166

The Bill will also establish a Deoxyribonucleic acid (DNA) Profiling Board responsible for prescribed functions, including specifying the list of instances for human Deoxyribonucleic acid (DNA) profiling and the sources of collection, enumerating guidelines for storage and destruction of biological samples, and laying down standards and procedures for establishment and functioning of Deoxyribonucleic acid (DNA) laboratories and Deoxyribonucleic acid (DNA) Data Banks. The board will also make recommendations for

privacy protection laws, practices and regulations relating to the access and collection of Deoxyribonucleic acid (DNA) samples.\textsuperscript{167} Although the Bill of 2012 is better than the Bill of 2007, it is still missing critical safeguards and technical standards essential to preventing the misuse of Deoxyribonucleic acid (DNA) and protecting individual rights.\textsuperscript{168}

Following are some shortcomings of the Bill of 2012:

- The Bill relies on the policy that the Deoxyribonucleic acid (DNA) analysis is infallible.\textsuperscript{169} It means that the Bill presupposes that the whole genetic analysis is flawless. It seems that the Bill has totally ignored the occurrence of false matches, cross-contamination, laboratory error and other limitations of forensic Deoxyribonucleic acid (DNA) analysis.\textsuperscript{170}

- The definitions given under the Bill of 2012 are very expansive. Moreover, the new Bill (Section B) further adds a variety of additional offences under special laws ranging from the Medical Termination of Pregnancy Act to the Motor Vehicles Act and empowers the Board to add any new law it wants to the Schedule. Section C of the Schedule identifies a wide variety of civil matters to be included in the Schedule including disputes related to paternity, pedigree, and organ transplantation. It reflects that the government is planning to conduct genetic testing on almost anyone in any way connected with even minor infractions of the criminal law or involved in virtually any civil proceeding.\textsuperscript{171}

- The definition of “offender” (Section 2y) is not limited to convicted criminals. Section 2y provides, “Offender means a person who has been convicted of or an under trial charged with a specified offence.”\textsuperscript{172} Section 2zi defines...
“suspect” as “a person suspected of having committed an offence.” It means that any person who has been arrested rightly or wrongly will have to be subjected to the genetic analysis.

- Section 2zo defines volunteers as “a person who volunteers to undergo a Deoxyribonucleic acid (DNA) procedure and, in case of a child or incapable person, his parent or guardian having agreed…” However, the Bill provides no clarity on the issue of the informed consent of volunteers.

Such a broad and expansive definitions of victim, offender and suspect allow the law enforcement agencies to conduct genetic testing on anyone, whether innocent or not. There is simply no corollary in any other country to such expansive authority. The Bill places India far outside the mainstream of policy in this area and raises serious and far ranging human rights concerns.

The researcher questions that what purpose the panoptican Deoxyribonucleic acid (DNA) database will achieve. It seems that the government has stopped believing its citizens, and every person is a suspect for the government. Furthermore, the researcher views that the mechanism for retaining the suspects' Deoxyribonucleic acid (DNA) samples and profiles is not clear in the Bill of 2012.

The Bill is also missing important provisions that would be necessary to protect the rights of the individual. For example, individuals are not permitted a private cause of action for the unlawful collection, use, or retention of Deoxyribonucleic acid (DNA), and individuals do not have the right to access their own information stored on the database. These are significant gaps in the proposed legislation as it restricts the rights of the individual.

It is submitted that following best practices be adopted in the Indian Deoxyribonucleic acid (DNA) profiling legislation:

- It should be ensured that notification is given to an individual if his/her information is legally accessed or shared.

---

173 Id., s. 2(zi).
174 Id., s. 2(zo).
• It is very necessary to take informed consent in the cases of volunteers, missing persons (or their families), victims, and suspects. And compulsory genetic testing should be ordered by the court only in the case where the law enforcement agencies are showing probable cause, and Deoxyribonucleic acid (DNA) evidence is directly relevant to the case.

• The individuals should have right to access and review their Deoxyribonucleic acid (DNA) files or databases. Children, victims, and missing persons should have right to request that their profile be deleted from the Deoxyribonucleic acid (DNA) database.

• The Deoxyribonucleic acid (DNA) profiles should not be used or retained for unlawful or unauthorized purposes. Moreover, the law should also be clear on the retention of the Deoxyribonucleic acid (DNA) specimens.

• Unauthorized persons should not have access to the Deoxyribonucleic acid (DNA) profiles. Every access should be authorized by the court only. Especially, persons like employers, insurance companies, etc. should be prohibited to conduct any genetic testing on their respective subjects. For this, it is also required that only government authorized or licensed registered medical practitioners should have power to conduct every genetic testing (after court’s approval only). It will also be helpful in regulating the admissibility of the Deoxyribonucleic acid (DNA) evidences in the family courts’ disputes.

• The purpose of the Paternity tests or genetic testing should not be to bastardise the children.

• Since negligent and deliberate malfeasance (e.g. false matches, etc.) in forensic laboratories cause injustice to the innocent, the authorities or the board ensure the quality of forensic laboratories, and the quality standards.

• The individuals should have right to bring a private cause of action against the unlawful storage of private information in the national, regional, or state Deoxyribonucleic acid (DNA) database. Obviously, it
will be a great check against the unlawful collection, analysis, and storage of genetic information.

- The greater clarity is required on the separation of convicted persons’ data from other persons’ like suspect, volunteers, children, missing persons, etc., databases.
- Again, the law must be made clear on the issue of familial searches in India.

12.2.10 Regulations on Closed Circuit Television (CCTVs) Cameras are Required

The researcher argues that what is the necessity of installing cameras at all places. The situations are not so worse that every place is a crime prone spot. Every installation demands strong justified reasons. However, the researcher observed that cameras have been installed unjustly at many places. For example, many students have view that they feel very uncomfortable with the installation of cameras in their school, college, or university canteens as these spots are places of solace for them. Similarly, the substantial number of population in Chandigarh refused to accept that installation of Closed Circuit Television (CCTV) cameras reduced the commission of crime in the city. Obviously, public opinion is insisting the government and the law enforcement agencies to recheck the utility of their surveillance devices or techniques.

Moreover, the researcher observed that majority of Closed Circuit Television (CCTV) cameras are operated illegally or in unregulated ways. For example, the unauthorized persons have easy access to the recordings of Closed Circuit Television (CCTV) cameras, and camera control operators use to watch the recordings for satisfying their prurient tastes or erotic desires. Similarly, people have installed the cameras at their shops, restaurants, hotels, etc. without following any privacy guidelines.

The researcher recommends adopting England’s “Surveillance Camera Code of Practice, 2013”, which prescribes following guiding principles for Closed Circuit Television (CCTV) camera operators:177

- Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

• The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

• There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.

• There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

• Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.

• No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.

• Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

• Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

• Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

• There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

• When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.
• Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

The researcher suggests that the camera control operators should be educated culturally, morally, legally, and technically. They should be sensitized towards individuals’ privacy rights. In addition to, the whole Closed Circuit Television (CCTV) surveillance system should be made free from any kind of technical flaw. It means that the system should be protected from any unauthorized access. No one could copy the images or recordings or any other information from the system.

Again, every video surveillance system should adopt following methods: 178

• Cameras should only be installed in identified public areas where video surveillance is necessary to protect public safety, detect or deter, and assist in the investigation of criminal activity.

• Cameras should be used for monitoring the identified spaces only. Cameras should not be directed to look through the windows of adjacent buildings.

• Operators should not zoom or manipulate the camera to overlook spaces that are not intended to be covered by the video surveillance program.

• Cameras should not monitor the inside of areas where individuals generally have a higher expectation of privacy (e.g., change rooms and public washrooms).

• The public should be notified of video surveillance equipment locations. Similarly, names, addresses, and contact numbers of responsible persons (of video surveillance) should be published.

• Organizations should publish the rationale of video surveillance, its objectives and the policies and procedures on their websites or other public places.

• Reception equipment should be in a strictly controlled access area. Only controlling personnel, or those properly authorized in writing by those personnel according to the organization’s policy, should have access to the controlled access area and the reception equipment. Video monitors should never be in a position that enables public viewing.

It is submitted that the time has come to monitor the monitors i.e. camera control operators. Every individual has a right to know that how the camera control operators react and behave on that individual’s video recordings.

12.2.11 Conduct Rules for Mobile Camera Phone Users Should Be Passed By the Parliament

In 2006 the Mobile Camera Phone Users (Code of Conduct) Bill 2006 was introduced in Parliament, but has lapsed, and in 2010 the Right to Privacy Bill was proposed in Parliament, but has not been passed. The Mobile Camera Phone Users (Code of Conduct) Bill proposed to create a code of conduct regulating the use of mobile camera phones in public places. The Bill require all manufactures to build camera phones that either flash a light or emit a sound when being used, regulate the uses of camera phones at public places e.g. taking consent and ensuring that the individual is aware that a picture will be taken. Similarly, the Right to Privacy Bill 2010 proposed that manufacturers should produce mobile phones with cameras which emit a sound of at least 65 decibels and flash a light at the time of taking picture. Digital recordings of individuals are prohibited without consent if the recording is of an unclothed body part, the recording is in a public place, or of a couple in a private place with the intent of blackmail or making commercial gains. However, the Bills were not approved by Parliament. Thus, unregulated use of mobile phones has led to a worse situation where it is unclear when and where mobile phones with cameras can be used, and how the recorded information can subsequently be used i.e. can it be uploaded to Face book or YouTube without prior permission.179

The mobile phone is a paradoxical device. Its primary function is social i.e. to enable its owner to communicate with other people. At the same time, though, using a mobile phone can seem profoundly anti-social, not least to people in the immediate vicinity. In restaurants, theatres and museums, on trains, or even standing in the supermarket checkout queue, there is no escape from chirping and bleeping phones, nor from the inane conversations of their owners. Therefore, many mobile phone design companies are intending to make “social mobiles”, which would modify their users’ behavior to make it less disruptive. For example, a phone is intended which would give its user a mild electric shock, depending on how loudly

the person at the other end is speaking. This encourages both parties to speak more quietly, otherwise the mild tingling becomes an unpleasant jolt.\textsuperscript{180}

Following are some terms of Ethics Code, which are being adopted by many governmental and non-governmental organisations for regulating the behaviour of mobile users:\textsuperscript{181}

\begin{itemize}
\item The mobile phone technology is considered one of the greatest technologies that emerged in the last few years to serve humanity, so do not ever use it to annoy or tease others.
\item Don’t call others during their times of sleep or rest.
\item Don’t get excited on receiving a wrong number and be more tolerant.
\item Check the number before dialing it in order not to annoy any person.
\item Don’t annoy others with your loud conversations in case you have a mobile phone’s loud speaker. Moreover, this offends the person you are talking to (on the mobile) as he does not know that others are hearing his conversation.
\item Don’t use mobile phones with high technologies such as the photographic or video cameras to violate others’ privacy. Know for sure that making materials that concern any person available on the Internet or mobile phones without his knowledge or consent is considered an immoral act punished by law and condemned and rejected by religion and moral ethics.
\item Avoid sending short message services (SMSs) that include inappropriate words or indecent photos as you will be charged and accused legally for this.
\item Don’t speak loudly on your mobile phones in public places such as hospitals, clinics or conference halls, etc.
\item Switch off your mobile phone in places of worship, lecture and examination rooms, cinemas, theatres, etc.
\item Switch off your mobile phone in hospitals especially in Intensive Care Units (ICUs) lest any potential wave interference occurs.
\item Choose a non-annoying ringtone for your mobile phone. Always remember that ringtones aim mainly to make the mobile user know that he has got a call.
\end{itemize}

\textsuperscript{180} Tom Standage (Ed.), \textit{Future of Technology}, 177 (2005).
\textsuperscript{181} National Telecom Regulatory Authority, “Mobile Phone Usage Ethics Code,” available at http://www.tra.gov.eg/presentations/crpc/Mobile_Usage_Ethics_Code_En.pdf accessed July 20, 2013, at 1:00 p.m. IST.
• Don’t use your mobile phone while driving as this will expose you to huge dangers and it is illegal.
• Use your mobile phone to report something or receive important information.
• Beware of dealing with the companies that defraud people concerning certain ringtones or applications for their mobile phones. You should deal only with trustworthy companies.
• Don’t respond to text messages or calls you receive from unknown numbers or sources because most probably they aim to swindle on you.
• On receiving a text message, verify the information mentioned in it before circulating it in order not to take part in the circulation and propagation of rumors or unverified information.

12.2.12 Comprehensive and Strong Data Protection Legislation is Required in India

The ‘Directive 95/46’ of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data’ (Data Protection Directive 95/46/EC) was established to provide a regulatory framework to guarantee secure and free movement of personal data across the national borders of the European Union member countries, in addition to setting a baseline of security around personal information wherever it is stored, transmitted or processed.\(^{182}\)

The Directive gave some globally accepted principles which are as follows:

• Legitimacy-defining when personal data processing is acceptable.
• Purpose restriction-ensuring that personal data is only processed for the purposes for which it was collected, subject to further consent from the data subject.
• Security and confidentiality- specifically by requiring the data controller to take appropriate technical and organisational measures.
• Transparency-that appropriate levels of transparency are provided to data subjects.
• Data subject participation-ensuring that the data subjects can exercise their rights effectively.

• Accountability- that those processing personal data would be held accountable for their actions according to the Outcomes.\textsuperscript{183}

However, the European Union Data Protection Directive 95/46/EC failed to face new challenges of globalization and technological developments like social networks and cloud computing. Therefore, strong guidelines for data protection and privacy were required. On 25 January 2012, the European Commission unveiled a draft legislative package to establish a unified European data protection law. The package includes a draft ‘General Data Protection Regulation’ (GDPR) that will be directly applicable in all member states of the European Union (EU) replacing the patchwork of different data protection laws currently in force in the different member states. The proposed new European Union (EU) data protection regime extends the scope of the European Union (EU) data protection law to all foreign companies processing data of European Union residents. It provides for a harmonization of the data protection regulations throughout the European Union (EU), thereby making it easier for United States companies to comply with these regulations; however, this comes at the cost of a strict data protection compliance regime with severe penalties of up to 2 % of worldwide turnover. The European Commissioner for Justice, Fundamental Rights and Citizenship, Ms. Viviane Reding, in a speech at the Digital Life Design summit here in Munich on 23 January 2012 outlined that the European Commission’s proposal will give European Union (EU) companies a competitive advantage globally, as the Regulation would provide for a harmonized pan-European Union (EU) regulation, replacing the existing patchwork of 27 national regulations; an improvement of the current system of binding corporate rules for a save transfer of data outside the European Union (EU); a regime allowing better control over individual’s data.\textsuperscript{184}

Following are proposed Changes to the Data Protection Law: \textsuperscript{185}

• The European Union (EU) data protection regulation will also apply for all non-European Union (EU) companies without any establishment in the


\textsuperscript{184} “New draft European data protection regime to apply also to all US companies processing data of European residents,” Law Patent Group, February 2012, available at http://www.mlawgroup.de/news/publications/detail.php?we_objectID=227 accessed on December 20, 2012, at 1:00 p.m. IST.

European Union (EU), provided that the processing of data is directed at European Union (EU) residents.

- As a general rule, any processing of personal data will require providing clear and simple information to concerned individuals as well as obtaining specific and explicit consent by such individuals for the processing of their data (Opt-in), other than in cases in which the data protection regime explicitly allows the processing of personal data.

- The Regulation will make a safe transfer of data outside of the European Union (EU) (including the procession of data in clouds) easier in the event that the parties involved commit themselves to binding corporate rules.

- New privacy rights, including data subject’s ‘right of portability’ and the ‘right to be forgotten’, will be established in the European Union. The ‘right of portability’ will allow a transfer of all data from one provider to another upon request, for example transfer of a social media profile or email, whereas the ‘right to be forgotten’ will allow people to wipe the history clean.

- The processing of data of individuals under the age of 13 will in general require parental consent, which will make it more difficult for companies to conduct business which is aiming at minors.

- All companies will be obligated to notify European Union data protection authorities as well as the individuals whose data are concerned by any breaches of data protection regulations or data leaks without undue delay, that is within 24 hours.\(^\text{186}\)

The E-Privacy Directive supplements the Data Privacy Directive, replacing a 1997 Telecommunications Privacy Directive, and providing a minimum standard for European Union member state regulation of commercial solicitation by means of email and telecommunications technologies.\(^\text{187}\) Article 13 of the E-Privacy Directive sets forth a basic rule of ‘opt-in’ consent for ‘unsolicited communications’: automated telephone calls, faxes, texts, and email. With respect to unsolicited commercial emails, an exception is created in

\(^{186}\)“New draft European data protection regime to apply also to all US companies processing data of European residents,” Law Patent Group, February 2012, available at http://www.mlawgroup.de/news/publications/detail.php?we_objectID=227 accessed on December 20, 2012, at 1:00 p.m. IST.

Article 13(2) for cases where a business has provided a good or service to an individual previously, the individual has provided his/her email, and an unsolicited email is sent to advertise ‘similar’ goods or services. Unsolicited emails sent under this exception must, however, provide the customer with an opportunity to ‘opt-out’ of future emails. Article 13(4) prohibits the sending of commercial emails that disguise or conceal the identity of the sender.\(^{188}\)

In 2006 and 2009, the E-Privacy Directive was amended as part of a wide-ranging initiative to create a ‘Telecoms Package’: a comprehensive regulatory framework for electronic communication and telecommunications. Part of this Telecoms Package involved the creation of a Body of European Regulators for Electronic Communications (‘BEREC’). The purpose of Body of European Regulators for Electronic Communications (‘BEREC’) is to facilitate institutional coordination of ‘national regulatory authorities’ (NRAs)-i.e. the regulatory bodies of European Union member states - and it therefore is intended to supplement the regulatory framework for electronic communications established by Directive 2002/21/EC (the regulatory ‘Framework Directive’).\(^{189}\)


Article 13 provides:

Unsolicited communications

1. The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.

2. Notwithstanding paragraph 1, where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use.

3. Member States shall take appropriate measures to ensure that, free of charge, unsolicited communications for purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2, are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications, the choice between these options to be determined by national legislation.

4. In any event, the practice of sending electronic mail for purposes of direct marketing disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease, shall be prohibited.

5. Paragraphs 1 and 3 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected.

According to The Hindu newspaper, the European Union and India have been trying to finalise their Broad-based Trade and Investment Agreement since 2006, with the goal of breaking down trade barriers, but progress in the past few months has been slow. India requested that the country should be recognised as a ‘data secure destination’, an accreditation which could increase the country’s outsourcing revenue from the European Union from $20bn to $50bn, according to Nasscom’s Data Security Council of India. Although the European Union Justice Department’s study into India’s data protection regime has not yet been completed, mutterings suggest it has identified significant gaps in local laws which could require time-consuming legislative amendments.  

Information Technology Act Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules 2011 should also add following recommendations:

- If a data breach occurs, affected individuals must be notified immediately.
- If information is legally accessed, the access must be notified at the close of the investigation.
- Any changes in a body corporate privacy policy should be notified to the public and the individual.
- Process to access and correct: At the time of collection body corporates must provide notice of the processes available to data subjects to access and correct their own personal information.
- For every mandatory collection of information, it is necessary to adopt National Privacy Principles. And such should be anonymized within one year if published in public databases.
- Personal data collected and processed by an organization must be adequate and relevant to the purposes for which they are processed.
- Every change in purpose must be notified to the data subject.
- Personal information must be used for the identified purpose only. After its use, the information must be destroyed as per the identified procedures.

---

190 Phil Muncaster, “ EU Justice Department stalls India's security clearance Without a 'data secure destination' cert India's locked out of $30bn euro-sourcing market,” The Register, 19th June 2013. Available at http://www.theregister.co.uk/2013/06/19/india_outsourcing_data_security_woes_eu/ accessed July 20, 2013, at 1:00 p.m. IST.

• If the government retains the data then it is mandatory on their part to follow National Privacy Principles.
• Data subjects should be able to confirm that an organization holds or is processing information about them.
• Data subjects should be able to obtain a copy of the personal data undergoing processing.
• Access to the information should always be made limited unless there are some compelling reasons.
• Whenever Body corporate provides information to third party, it is necessary on their part to provide notice of such disclosure to the data subject.
• It must be made mandatory for third parties to observe the National Privacy Principles.

National privacy principles require notice, choice and consent, collection limitation, purpose limitation, access and correction, disclosure of information, security, openness, and accountability. The National Privacy Principles have been envisioned as being applicable across sectors, legislation, policy, projects, and bodies in order to broadly harmonize privacy protection in India and address and readily adapt to emerging and changing technologies and practices.\(^{192}\)

It is suggested that the upcoming Privacy Act in India should also devise a system of co-regulation through self-regulating organizations (SROs) and their member organizations to remedy privacy violations. The Act should prescribe the stringent punishments for privacy violations. At the same time, the Privacy Act should also prescribe list of exceptions to the right of privacy. The framework should enable quick redress by allowing individuals to resolve their complaints through alternative dispute mechanisms (ADRs), the Privacy Commissioner, or the Courts. Once the Privacy Act is approved by Parliament, the regulatory bodies in the Act should be accountable to Parliament.\(^{193}\)

The revelation of PRISM program in the US has reignited global debate on national security versus right to privacy. Many governments’ programs for national security and cyber security raise privacy concerns. It is the responsibility of the governments to assuage such concerns by establishing adequate safeguards for protecting privacy. In this context it is appreciable that one of the objectives of National Cyber Security Policy (NCSP – 2013) is to enable safeguarding of privacy of citizen’s data, even though no specific strategy or activity

\(^{192}\) Id., at 69.
\(^{193}\) Id., at 56.
to achieve this objective has been mentioned in the policy. A commendable job has been done by the government by bringing a comprehensive cyber security policy. The road ahead in terms of defining the implementation plan will be an arduous task. The due diligence for defining the plan must take into consideration the possible implications—positive and negative both—of each policy statement.
