SUMMARY OF THE THESIS

On our planet, all living organisms are blessed with a sense of self-protection. Depending upon their capacity, every living organism possesses natural power to protect themselves from any bodily harm. Their natural resistance power does not allow anybody to intrude into their physical privacy. Therefore, it would not be incorrect to say that physical privacy is born with the birth of all living beings. However, it is submitted that human beings are blessed with some extraordinary senses. It is only for this reason that human beings have developed their standards for preserving ‘privacy rights’. In order to achieve the present version of “Privacy”, a man has been fighting since pre-historic times. Starting with tangible claims, human beings fought for their honour, reputation, and feelings. During this sacred journey, human beings witnessed the great shift from mere physical privacy to mental or psychological privacy. Consequently, the shift widened the scope of privacy. Currently, the concept of privacy includes multiple types of privacy interests like 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.\(^1\) Another reason behind the development of the concept lies in the importance of ‘privacy.’ Right to privacy helps an individual in creating conducive ambience for knowing about his or her spiritual existence. Private space is further required for possessing any idea or opinion. Again, ‘privacy values’ are also the basic pillars of our democratic set up since privacy ensures one’s speech and expression, freedom of association, 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’.\(^2\) Furthermore, it is pertinent to mention here that scientific developments played significant role in the growth of the concept of privacy since the developments brought dynamic changes in the living conditions of all human beings. The advanced features of sophisticated technologies fascinated people, and allured them to be dependent on their use. It made people’s lives more convenient. But at the same time, people also started misusing the intrusive characteristics of the sophisticated technologies for many unlawful purposes. Irresponsible media did not miss the chance of using intrusive technologies for disseminating sensational news. Media’s intrusive actions violated individuals’ private lives, and ignited the debate of freedom of media and privacy. It has been observed that a commercially oriented media’s over-inquisitive attitude and an unethical

\(^2\) Ibid.
competition in the field of journalism compel the journalists to report sensational news by intruding into individuals’ private lives. Again, privacy advocates have shown their great concern for individuals’ privacy rights against increasing surveillance powers in the contemporary society. The governments’ extensive gatherings on individuals’ personal information after the 9/11 United States and 26/11 Mumbai attacks have created an imbalance in the relationship of privacy and security. Obviously, the imbalances affecting fundamental freedoms weaken every democratic set up. In the present technological world, both public and private agencies have devised unprecedented techniques for monitoring people. Not surprisingly, ubiquitous surveillance compels an individual to behave against his normal behaviour. It prevents an individual to make his or her own ideas or opinions; to make his or her selective associations or groups; to speak unknowingly; to take his or her autonomous decisions, etc. Similarly, the sophisticated mobile cameras are in the hands of every individual in the society. It has been observed that mobile camera users are hardly sensitized towards others’ privacy rights as there is non-availability of any conduct rules for the users. Similarly, the prevailing legislations are inefficient to regulate monitorings conducted by camera control operators. Increasingly, new media tools are being misused at many other fronts, which have been discussed in this Thesis. Moreover, the government has not yet made any policy on social media. Rather, social networking sites have become another mode of surveillance for the governments. It has been revealed that the executive agencies compel the social networking sites to remove any dissent material from their web pages.3

The whole research work has been conducted to fulfill following objectives:

• To analyze the value of Privacy among individuals.
• To analyze the awareness of privacy rights among people.
• To analyze usages of excessive surveillance techniques both by public and private agencies.
• To analyze unregulated uses of technologies having potential to invade individuals’ privacy.
• To analyze the power and responsibility of the government in the process of whole surveillance system.
• To analyze the tussle between freedom of media and privacy rights.
• To analyze role of social networking sites in the present information society.

3 “Google Transparency Report, 2012” available at http://www.google.com/transparencyreport/removals/government/ accessed on April 9, 2013, at 5:00 p.m. IST.
• To analyze the modes and uses of collection of personal information by private bodies.
• To study the role of judiciary in recognizing different facets of right to privacy in India.

The present research work required both theoretical and empirical study. The theoretical work dealt with the literature relating to value and importance of privacy attached to different cultures or societies, media and technologies intrusion in individual privacy, protection of right to privacy by constitution, legislative measures or some other government policies, and international conventions and treaties with respect to the protection of individual privacy. The empirical work comprised of the questionnaires in order to bring out the actual factors and forces behind the practice of data collection by the government and other private authorities and to find out the views about the value of privacy among various sectors of the society.

The above said problems have potential to affect anybody’s private life, irrespective of his or her belongingness to rural area or urban area. The researcher adopted Union Territory of Chandigarh as the area of the present study. Here, people are more aware than other places about our study. People are strongly dependant on new media and internet communications, and are subjects of various modes of surveillance including electronic, physical, data, and psychological. The empirical research has been conducted by administering the questionnaires. The researcher collected and analysed the data of five hundred respondents from five different categories i.e. students, advocates, journalists, public officials, members of general public.

Considering the current issues, the researcher has classified the thesis into Twelve Chapters. In Chapter 1, the researcher has mentioned introductory part of this research work. Chapter 2 investigates the concept of privacy historically, starting with the ancient Greek and Roman literature. The Chapter also gives references about philosophical, sociological, and anthropological studies of privacy. The Chapter also includes the studies regarding traces of private life in tribal societies. In the mid part of the Chapter, Indus civilization’s recognition to privacy has been discussed. Architecture of the houses and streets in Indus civilization reflect their expectations for privacy. The concept of privacy has also been found in the ancient Hindu scriptures. The Chapter also gives references of various other religious scriptures including Islam and Sikhism, whose sacred texts acknowledge the
importance of privacy in the spiritual journey of all human beings. In the later part of the Chapter, the courts’ recognition to privacy values in the British India has been discussed.

Chapter 3 describes meaning, nature and scope of the concept of right to privacy. The Chapter starts with philosophical discussions of eminent philosophers like Aristotle, John Locke, J.S. Mill, Samuel Warren and Louis Brandeis. The Chapter covers viewpoints given by critiques, reductionists, and coherentists of privacy. The Chapter gives references of some judgements and authors’ viewpoints who understand privacy as a cluster concept covering interests in 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.

Chapter 4 includes the Constitutional provisions protecting right to privacy in India. The Chapter also highlights some important provisions of the Indian Penal Code, 1860, which impose penal sanctions on actions or omissions that constitute a violation of privacy rights. Provisions of the Code of Criminal Procedure, The Narcotic Drugs and Psychotropic Substances Act, 1985 and Income Tax Act, 1995 regarding search and seizure have been mentioned. In order to understand data privacy in India, the researcher strive to analyse various legislations like Information Technology Act, 2000, Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, The Information Technology (Guidelines for Cyber Cafe) Rules 2011, The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, The Information Technology (Intermediaries guidelines) Rules, 2011, The Privacy (Protection) Bill, 2013, etc.

In Chapter 5, the International perspective of the concept of right to privacy has been mentioned. The Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 (the Directive) has been considered as 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. 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. Even if data is being transferred outside of European Union (EU)

---

member countries, protection should be given to such data. Furthermore, personal data is barred from transferring to a third country who doesn’t have an adequate law on privacy protections.\(^7\) 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.\(^8\) The Directive prohibits European Union (EU) member states from collecting data that reveal an individual’s ethnic origin, race, political conviction, religious beliefs, or health and sexuality.\(^9\) 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.\(^10\)

However, the European Commission noticed that due to advancement in rapid technological developments and globalization have brought new challenges for the protection of personal data. The commission observed that technology and social networking sites has made easy for 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.\(^11\) Although the European Union Justice Department’s study into India’s data protection regime has not yet been completed, mutterings suggest it has

---


\(^11\) Ibid.
identified significant gaps in local laws which could require time-consuming legislative amendments.\textsuperscript{12}

In Chapter 5, the researcher also endeavoured to trace history of privacy in United States and United Kingdom. The United States’ courts have developed privacy rights on a constitutional basis. Various amendments of the American Constitution like First, Third, Fourth, Fifth, and Fourteenth Amendments containing provisions protecting privacy interests has laid the necessary foundation for the courts in this regard. These amendments mainly protect informational privacy.\textsuperscript{13} 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 sexuality, search and seizure, eavesdropping (4) Data protection and press.\textsuperscript{14} In 1977, the United States Supreme Court claimed in \textit{Whalen v. Roe},\textsuperscript{15} 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.\textsuperscript{16}

The Privacy Act of 1974 establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual. The Privacy Act requires that agencies give the public notice of their systems of records by publication in the Federal Register. The Privacy Act prohibits the disclosure of a record about an individual from a system of records absent the written consent of the individual, unless the disclosure is pursuant to one of twelve statutory exceptions. The Act also provides individuals with a means by which to seek access to and amendment of their records, and sets forth various agency record-keeping requirements.\textsuperscript{17}

\textsuperscript{12} 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 \url{http://www.theregister.co.uk/2013/06/19/india_outsourcing_data_security_woes_eu/} accessed July 20, 2013, at 1:00 p.m. IST.
\textsuperscript{14} \textit{Id.}, at 53.
\textsuperscript{15} 429 U.S. 589 (1977).
\textsuperscript{16} \textit{Id.}, at 598-600.
\textsuperscript{17} Available at \url{http://www.justice.gov/opcl/privacyact1974.htm} accessed on April 30, 2012, at 5:30 p.m. IST.
As the researcher noted in the Chapter 5, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) has enhanced the powers of law enforcement agencies to access personal records held by libraries, health insurance companies, bookstores, schools, businesses, and civil or non-profit organizations. With the passage of this Act, Fourth Amendment of United States’ Constitution has also been diluted. Thus, it has become easier for law enforcement agencies to obtain personal records from financial institutions, telephone companies, and Internet service providers.18

The Chapter 5 also contains the status of privacy in the United Kingdom. In the United Kingdom, the law of privacy has been developed through rule of ‘breach of confidence,’ the Human Rights Act 1998, and the Data Protection Act 1998. Recently, Justice Leveson found that the current systems of both internal governance in some parts of the press, and industry self-regulation of the press, have not worked and are not working.19 The present Press Complaints Commission (PCC) lacks the independence that is critical to building public confidence in a regulator.20 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.21

In Chapter 6, the concept of surveillance has been discussed in detail. The opening pages of the Chapter refer the George Orwell’s ‘Big Brother Society,’22 Bentham’s ‘Panoptican,’23 and Michel Foucault’s ‘Bio Power,’24 as metaphors of current surveillance

---

20 Id., at 1749.
21 Id., at 1759.
23 Bentham’s Panopticon is, for Foucault, an ideal architectural model of modern disciplinary power. It is a design for a prison, built so that each inmate is separated from and invisible to all the others (in separate “cells”) and each inmate is always visible to a monitor situated in a central tower. Monitors will not in fact always see
society. For better understanding, the researcher has classified the modern techniques of surveillance in the categories of physical surveillance technology, electronic surveillance technology, psychological surveillance technology, and data surveillance technology. Furthermore, unreasonable search and seizure is a part of this Chapter. The historical value of rights against unreasonable searches has been discussed in detail, including the important case laws of common law and United States’ Supreme Court. The Chapter also includes the role of Indian judiciary in protecting the right to privacy against the unreasonable searches and seizures in India. In this Chapter, the researcher also endeavoured to analyse the judicial attitude in India towards the admissibility of evidences, which have been collected illegally.

Considering electronic surveillance technologies, the researcher mentioned in the Chapter 6 that the Closed Circuit Television (“CCTV”) cameras have been installed almost everywhere in the society like villages, schools, hospitals, crèche, schools, office, home, etc. The cameras’ role is to protect the society from different crimes, for example, the purpose of installing cameras on the roads is to capture rowdy vehicles. The inherent characteristics of Closed Circuit Television (“CCTV”) cameras, i.e. recording or storing the images and videos, have the significant ability to affect people’s rights. Among numerous rights, the right to be different, the right to hope for tolerant forgiveness or overlooking of past foolishness, errors, humiliations, or minor sins (notion of the possibility of redemption), and right to make a fresh start will also be jeopardized.

The researcher noted in the Chapter 6 that the problem becomes more aggravated if the monitoring of such videos is being done in an unregulated way. The person, who is watching live videos of Closed Circuit Television (“CCTV”) cameras, may record images or videos for his own private purposes or to satisfy his erotic desires. Indeed, it is mandatory to maintain a register in which entries of every human monitor should be recorded. Moreover, the camera control operators should be educated morally, culturally, technically, and legally. Every kind of loophole, which let watchers to carry away recordings with them, should be removed. There are some other instances, like installation of hidden cameras in the trial of each inmate; the point is that they could at any time. Since inmates never know whether they are being observed, they must act as if they are always objects of observation. As a result, control is achieved more by the internal monitoring of those controlled than by heavy physical constraints. Gutting, Gary, “Michel Foucault,” in Edward N. Zalta (ed.), The Stanford Encyclopedia of Philosophy (Summer 2013), available at http://plato.stanford.edu/archives/sum2013/entries/foucault/ accessed on July 16, 2012 at 1:30 p.m. IST.

24 Biopower, for Foucault, is a technique “for achieving the subjugations of bodies and the control of populations.” Michel Foucault, The History of Sexuality, Vol. 1, 140 (1976).


rooms of shopping malls to prevent shoplifting, which are moving us to the naked society. Installation of cameras in bedrooms, restrooms or trial rooms is violation of an individual’s reasonable expectation of privacy. Increasingly, the recent incidence of leakage of the Delhi metro train Closed Circuit Television (“CCTV”) footage has again narrated the story of the unregulated use of Closed Circuit Television (“CCTV”) camera recordings. It was reported that Closed Circuit Television (“CCTV”) cameras installed in Delhi Metro trains have been used to capture couples' intimate moments. Moreover, the video footage captured has also been uploaded on pornographic sites. It was also reported that 13 videos have been uploaded on porn sites and these have been viewed by nearly 1.5 lakh people. It is believed that many such videos have been made but are yet to come in public domain.27

Meanwhile, many political leaders alleged that the government tapped their phone for political purposes.28 Therefore, illegal access to individuals’ records to know their political association, opinions, views or any other expression has raised substantive questions against the governments’ claim to protect individual privacy.

Edward Joseph Snowden, the 29-year-old former National Security Agency (NSA) contractor leaked the highly classified secrets of United States Intelligence system. The leaked documents revealed a massive program to compile United States telephone records into a database for antiterrorism and counterintelligence investigations. Another program, called Prism, had given the National Security Agency (NSA) access to records at major online providers like Google, Facebook and Microsoft to search information on foreign suspects with court approval. The secret program had been under way for many years.29 At the same time, it is pertinent to note that the Unique Identification number (UID) Authority has selected three United States companies—one for supporting and two for creating the data repository—without taking into consideration the fact that these United States companies are duty bound to furnish their data if asked for by the United States government.30 The whole situation may put Indians’ personal information at stake.

---

30 “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.
Chapter 6 also highlights about one’s freedom of speech and expression on social networking sites. 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.31 The indicting statistics show the Indian government ranks third in requesting users’ data since July 2009, when Google started indexing the requests. It was also the second snoopiest government in the world in the first half of previous year i.e. in 2012. The report revealed that Google also received requests from unauthorized agencies for the removal of content. Such disclosure reflects surreptitious censorship on the part of executive authorities.32

Chapter 7 of the thesis focuses on the protection of an individual’s personal information in the present technological world. Personal data on all individuals have become an indispensable ‘raw material’ for countless government and private organizations, crucial products, services, performances, and responsibilities.33 In recent years, the private sector has shown the greatest innovation in these respects. Medical care increasingly involves complex, multi-channel flows of information on matters ranging from the patient’s medical history and genetic inheritance to his insurance status. Credit and banking require constant accessing of account balances, recent transactions, credit history, and available credit. The sale and use of all forms of insurance are predicated on close assessment of risk and reward, cost and benefit—all requiring analysis of the experience of identifiable individuals. Marketing, in its many forms, involves analytical monitoring of consumers’ product choices and advertising susceptibilities.34 But at the same time, these developments have endangered many privacy rights. In this Chapter, the privacy issues of the present information age have been explored.

Judith Wagner Decew emphasized that information about one’s daily activities, personal lifestyle, finances, medical history, and academic achievement, whether written or not, part of a public record or not, may be viewed by an individual as information he or she

31 “Google Transparency Report,” available at http://www.google.com/transparencyreport/removals/government/ accessed on April 9, 2013, at 5:00 p.m. IST.
34 Ibid.
need not divulge and can expect others to guard as well.\(^{35}\) Besides, Herman T. Tavani showed
great concern about informational privacy in computer/informational technology. Tavani says
that personal privacy can be analysed in terms of four factors— the amount of personal
information that can be collected, the speed at which personal information can be exchanged,
the duration of time that the information can be retained, and the kind of information that can
be acquired.\(^{36}\)

The computer-born revolution in man’s capacity to process data is obviously an
enormous boon. In business, government, medicine, science, and a dozen other fields, men
are now able to make more fact-based, more logical, and more predictable decisions than they
could do before the age of electronic information storage and retrieval.\(^{37}\) The traditional
methods of gathering information have been replaced by the electronic digital computers. The
recent technologies have the capacity to store more records and manipulate them more
effectively and rapidly than was ever possible before.\(^{38}\) Every organization, by using giant
computers, collects information about its employees, clients, members, taxpayers, or other
persons in the interest of the organization.\(^{39}\) In the process of such collection, the government
makes dossiers on each individual’s personal information. The dangerous aspect of these
dossiers lies in the fact that the individuals hardly know about the existence of such dossiers.
They are also unaware of any content in those dossiers.\(^{40}\)

The process of Data mining involves an integration of techniques from multiple
disciplines such as database and data warehouse technology, statistics, machine learning,
high-performance computing, pattern recognition, neural networks, data visualization,
information retrieval, image and signal processing, and spatial or temporal data analysis.\(^{41}\) By
performing data mining, interesting knowledge, regularities, or high-level information can be
extracted from databases and viewed or browsed from different angles. The discovered
knowledge can be applied to decision making, process control, information management, and
query processing.\(^{42}\) With more and more information accessible in electronic forms and
available on the web, and with increasingly powerful data mining tools being developed and
put into use, there are increasing concerns that data mining may pose a threat to individual

\(^{36}\) Herman T. Tavani, “Informational Privacy: Concepts, Theories, and Controversies,” in Kenneth Einar Himma
\(^{38}\) Id., at 160.
\(^{39}\) Id., at 161.
\(^{40}\) Id., at 160.
\(^{41}\) Jiawei Han and Micheline Kamber, *Data Mining: Concepts and Techniques*, 9 (2010).
\(^{42}\) Ibid.
privacy and data security.\textsuperscript{43} Therefore, it is possible that the data of an individual’s personal information may be misclassified. A larger concern is the misapplication of data mining techniques. Data may also be used for unauthorized purposes.\textsuperscript{44}

However, the technology by itself doesn’t violate an individual’s privacy rather it’s the people using this technology and the policies they carry out that create violations.\textsuperscript{45} In order to reap the benefits of technology, it is more important to use technology to protect personal freedom.\textsuperscript{46} Therefore, it is necessary to regulate the technology. At the same time, the government should play prominent role in stopping technology and the free market from killing our privacy. Furthermore, the problem can also be diluted by way of making careful and informed consumers.\textsuperscript{47}

Eventually, Consumers are obvious stakeholders in the whole process of behavioral target marketing. Consumers do have the respect for their privacy. Their unwanted dissemination of information decreases lessens their sense of autonomy. Such intrusive selling disturbs their household peace.\textsuperscript{48} Paradoxically consumers don’t even know about the information they gave to the marketers.

Although it is not explicit, an individual always supplies information under this understanding that it will be used for particular purpose. If such information is being exhibited for any other purpose without his consent then it is a breach of the privacy one is entitled to expect, and an infringement of his right to choose.\textsuperscript{49}

Further, as soon as an individual subscribes himself with any Communications providers, like the telephone companies and Internet Service Providers, the latter collects the personal details of the former. The Internet Service Providers have access to certain kinds of transactional data. Whenever the individual downloads any software, calls anyone, sends or receives e-mail, upload videos, etc., the Internet Service Providers may make dossiers of such transactions.\textsuperscript{50}

In the present world, however, all public and private entities have the same source for accessing personal data. Common source is known as Data brokers who gathers, organizes

\textsuperscript{43} Id., at 679.
\textsuperscript{44} Patricia Oslund and Larry Hoyle, “Data mining”, in William G. Staples (ed.), \textit{Encyclopedia of Privacy}, 159-161 at 161 (2007).
\textsuperscript{46} Id., at 5-6.
\textsuperscript{47} Id., at 6.
and sells the data about individuals. Employers, lenders, marketers, insurance vendors, law enforcement agencies, and others buy such data from Data brokers as per according to their needs.\(^{51}\)

Chapter 7 also covers issue regarding right to privacy of public officials. While the Right to Information Act, 2005 gives the public right to access public documents, it also restricts disclosure of certain kinds of information.

In Chapter 7, the researcher endeavoured to analyse Privacy-Enhancing techniques for protecting personal data. Herbert Burkert defined Privacy Enhancing Technologies (“PETs”) as “technical devices organizationally embedded in order to protect personal identity by minimizing or eliminating the collection of data that would identify an individual or, if so desired, a legal person.”\(^{52}\)

Chapter 8 includes freedom of media and right to privacy. Freedom of speech and expression is not an absolute freedom as government may impose reasonable restrictions on its exercise by legislating on matters concerning libel, slander, contempt of court, any matter offending decency and morality, or which undermines the security of or tends to overthrow the state. The right to freedom of speech and expression and the right to privacy are two sides of the same coin. One person’s right to know and be informed may violate another’s right to be left alone. Just, as the freedom of speech and expression is vital for the dissemination of information on matters of public interest, it is equally important to safeguard the private life of an individual to the extent that it is unrelated to public duties or matters of public interest. The law of privacy endeavours to balance these competing freedoms.\(^{53}\)

The Chapter highlights practices of invading celebrities’ privacy. In the case of entertainment and sports stars, privacy invasions must be justified by showing that the expected benefits outweigh the potential harms of releasing private information and images of celebrities. The harm to celebrities from invasions of their privacy may include loss of self-determination and self-respect; loss of reputation, status, and revenue; emotional damage; and damage to meaningful relationships. Celebrities’ families may be similarly harmed.\(^{54}\)


Investigative journalism is a kind of journalism in which reporters deeply investigate a topic of interest, often involving crime, political corruption, or some other scandal.\textsuperscript{55} It is the responsibility of investigative journalists to make the citizens more informed about public interest. In order to fulfill such responsibility, they will have to cull out the hidden truth from government policies. In the whole process, ultimately people will receive the transparent and accountable government. On one hand, Sting Operation serves the public interest by strengthening the democratic framework by disseminating information about facts of vital interest to society that are not easy to obtain by simple requests or efforts. On the other hand, some recent incidents prove the misuse of Sting Operation by media and private entities to increase the channel viewership, settle political scores, harm corporate interests, malign reputation etc. Such Sting Operation that are carried on with ulterior motives not only harm the person and the institution trapped in the sting, but has the potential to shake people’s faith in the institutions and create a general atmosphere of cynicism in the society.\textsuperscript{56} Therefore, the Chapter introduces many media laws protecting individuals’ privacy. It also includes the role of Indian judiciary in case of censorship of films in India.

In Chapter 9, the role of Indian Judiciary in recognizing right to privacy has been discussed. For every peaceful society, sense of justice among the people is a pre-condition. A society without a sense of justice cannot be peaceful and cannot be called society at all, rather it would be considered as jungle. To express the human approach in a positive way it must be said that justice is absolutely necessary for ensuring peace and security in the society, in the country as a whole.\textsuperscript{57} For recognizing right to privacy in India, the judiciary has construed the concept of ‘life’, ‘personal liberty’ and ‘procedure established by law’ in a very liberal manner. The courts in India have also recognized prisoners’, women’s privacy rights, medical confidentiality and medical examinations, and decisional privacy in India. Recently, the Hon’ble Supreme Court of India has recognized one’s mental privacy.\textsuperscript{58} It is submitted that the Hon’ble Supreme Court of India emphasized on the procedural safeguards of the administration of such psychological tests. By recognizing one’s mental privacy, the court has broadened the horizon of right to privacy. It is pertinent to mention here that such a significant judgment is also a warning to the private individuals or bodies that are in practice of conducting such psychological tests over concerned subjects.

\textsuperscript{56} \url{www.lawcommissionofindia.nic.in/stingoperation.doc} accessed on December 4, 2010 at 11.48 p.m. IST.
\textsuperscript{57} Umeshwar Prasad Verma, \textit{Law, Legislature and Judiciary}, 82 (1996).
\textsuperscript{58} \textit{Selvi v. State of Karnataka}, 2010(4) SCALE 690.
Similarly, it is submitted that the courts do not feel any hesitation in recognizing individuals’ right of personal autonomy while construing the true spirit of the Constitution. The emerging issues of right to privacy are knocking the doors of Indian courts because of the fact that the prevailing legislations are insufficient to tackle the privacy issues. Therefore, it is the duty of the Indian judiciary to fill up every legislative gap by redressing privacy violations.

Chapter 10 contains data results. Chapter 11 provides an analysis of primary and secondary data. In Chapter 12, the researcher has summed up thesis with concluding remarks and suggestions.

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.
- 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.

Considering the above said findings, the researcher has submitted many suggestions.