EXPANDING HORIZONS OF RIGHT TO PRIVACY: A STUDY

Dissertation submitted to National Law University and Judicial Academy, Assam

in partial fulfilment for award of the degree of

MASTER OF LAWS

Submitted by

Himanshu Sharma

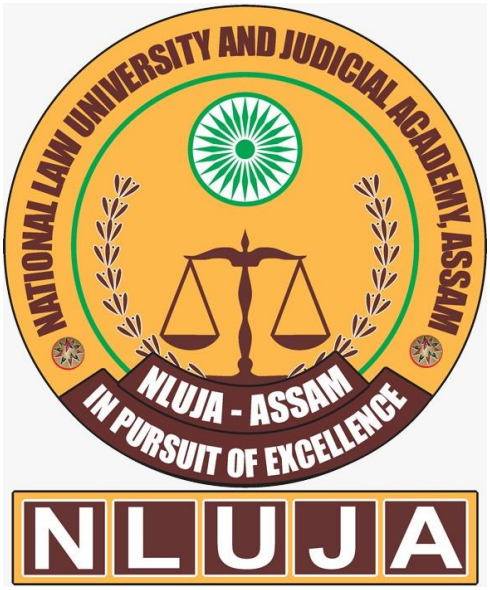
UID: SM0220035

LL.M. (2020-21) IInd Sem

Supervised by

Dr. Daisy Changmai

Guest Faculty of Law



National Law University and Judicial Academy, Assam

August, 2021

TABLE OF CONTENTS

CERTIFICATE

This is to certify that HIMANSHU SHARMA has completed his dissertation titled "EXPANDING HORIZONS OF RIGHT TO PRIVACY: A STUDY" under my supervision for the award of the degree of MASTER OF LAWS.

Date: 2 August, 2021

Place: Guwahati, Assam

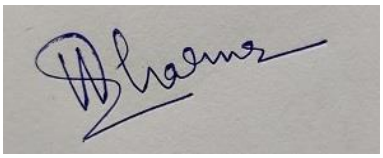
DR. DAISY CHANGMAI

Guest Faculty of Law

NLUJA, Assam

DECLARATION

I, HIMANSHU SHARMA, do hereby declare that the dissertation titled "EXPANDING HORIZONS OF RIGHT TO PRIVACY: A STUDY" submitted by me for the award of the degree of MASTER OF LAWS of National Law University and Judicial Academy, Assam is a bonafide work and has not been submitted, either in part or full anywhere else for any purpose, academic or otherwise.



Date: 2 August, 2021

Place: Guwahati, Assam

HIMANSHU SHARMA

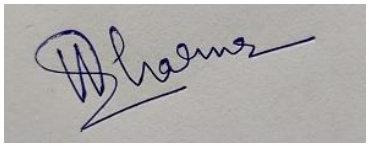
UID: SMO220035

NLUJA, Assam

ACKNOWLEDGEMENT

At the very outset, I would like to express my sincere and heartfelt gratitude to **Dr. Daisy Changmai (Guest Faculty of Law) National Law University and Judicial Academy, Assam** for her constant guidance, co-operation and encouragement which immensely helped me in completing my dissertation. This work would not have been possible, without the regular consultation and inputs provided by her. It is due to her patience and guidance that I have been able to complete this task within the time frame. I am highly obliged for her valuable advice, directions and kind supervision. Her sympathetic attitude, scholarly guidance and keen interest in the work have inspired me at every stage of my efforts with equal sincere feeling. Her sincere encouragement was tremendous moral support to me.

I would also like to thank my friends and family for giving me the constant support, motivation and encouragement throughout the work.



Himanshu Sharma

LL.M. (2020-21)

UID-SM0220035

PREFACE

Privacy is ambiguously defined, and bringing out the in-depth concepts from various related backgrounds have complicated this journey. According to Henry Campbell Black's Law Dictionary, *"determines the non-intervention of secret surveillance and the protection of an individual's information".*

Louis Brandeis J in a celebrated judgment has said that "*Right to privacy is 'the right most valued by civilized men"*. The technological age we live in today has its advantages as well as disadvantages . The positive face of the story is that the world has become more open to domestic and international exchanges; the downside is that this technological age has brought new ethical and legal challenges.

Nowadays, with the advancement of technology, adequate protection of privacy has become more and more important. Our lives are over-influenced by social media, so everyone must be protected individually. In some way, people don't have to worry about their right to privacy. As the Supreme Court regards this right as a basic right, the right to privacy becomes even more important. RTP got recognized as Fundamental Right under Indian Constitution.

Although privacy must be protected in all respects like other basic rights because it is recognized as Fundamental Right but however RTP is not absolute in nature and government may impose restrictions in certain specific circumstances.

This research paper attempts to explore the deep concepts of right to privacy, its recent development and prospects from different Constitutional angels. Researchers studied the protection of human personal data in the modern technological world, as well as media freedom and privacy rights. During the investigation with various topic researcher has made a doctrinal study with the theoretical analysis approach.

TABLE OF CASES

J

Justice K. S. Puttaswamy & Anr. v. Union of India & Ors, (2017) 10 SCC 1

K

K.J. Doraisamy v. The Assistant General Manager, State Bank of India, 2007 136 Comp. Cas 568 (Mad).

Kharak Singh v. State ofUP, AIR 1963 SC 1295.

M

M.P. Sharma v. Satish Chandra, AIR 1954 SC 300.

Mackinnon Mackenzie and Co Ltd v. Audrey D'Costa, AIR 1987 SC 1281.

Malak Singh v. State of Punjab, 1981 Cri LJ 320.

Maneka Gandhi v. Union of lndia, AIR 1978 SC 597.

Mr. Xx. Hospital 'Z\ AIR 1999 SC 495.

N

Naz Foundation v. Government of NCT of Delhi, 2010 Cri.LJ-94 (Del.).

Neelabati Bahera v. State ofOrissa, 1993 SCR (2) 581.

Neera Mathur v. LIC, AIR 1992 SC 392.

Navtej Singh Johar v. Union of India, (2018) 1 SCC 791

P

P. Rathinam v. Union of India, AIR 1994 SC 1844.

People’ s Union for Civil Liberties v. Union of India, AIR 1997 SC 568.

R

R. Rajagopal v. State ofT.N, (1994) 6 SCC 632.

R. Sukanya v. R. Sridhar, AIR 2008 Mad. 244.

S

Selvi v. State of Karnataka, 2010(4) SCALE 690.

Suchita Srivastava and Another v. Chandigarh Administration, AIR 2010 SC 235.

U

Union of India v. Association for Democratic Rights, AIR 2002 SC 2112.

V

Vishaka v. State of Rajasthan, AIR 1997 SC 3011.

X

X v. Hospital Z, AIR 2003 SC 664.

TABLE OF STATUTES

1. Indian Penal Code, 1860

2. Indian Contract Act, 1872.

3.Indian Telegraph Act, 1885.

4.Indian Constitution, 1950.

5.Code of Criminal Procedure, 1973.

6. Press Council Act, 1978.

7. Information Technology Act, 2000.

8.Right to Information Act, 2005.

9. Press Council of India Norms of Journalistic Conduct, 2010.

10. Juvenile Justice (Care and Protection of Children) Act, 2015.

11. Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016.

ABBREVIATIONS

AIR	All India Reporter
Art.	Article
CCTV	Closed Circuit Television
Ibid	In the same place
Id.	Idem (the same)
IPC	Indian Penal Code
IT	Information Technology
NCT	National Capital Territory
OECD	Organisation for Economic Cooperation and Development
RTI	Right to Information Act
RTP	Right to Privacy
SCC	Supreme Court Cases
S.	Section
Supra	above
TRAI	Telecom Regulatory Authority of India
UDHR	Universal Declaration of Human Rights
U. N.	United Nations
U. K.	United Kingdom
U.S.A.	United States of America
v.	verses

Chapter 1

INTRODUCTION

1.1 Background

The terms like 'privacy' and RTP are not easy to be critically analyse and understood. Privacy is majorly based on the theory of natural rights and usually seen to have a responsive approach towards latest information and communication technologies. RTP comes under the ambit of basic rights, hence it is granted to each and every individual the right to keep a private ambit around themselves which many consists of our body, personal lifestyles, feelings, Choices, likes, dislikes, home, bank balance details etc. Every individual is entitled with the right to decide upon that how much others can peep into their privacy ambit and how much their private information should come into public Domain. 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. At present, the privacy concept consists of many forms of privacy like Managing facts about oneself, restricting physical and mental access to oneself, and controlling one's ability to make critical family and lifestyle decisions in order to be self-expressional and build diverse relationships are just a few examples.[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. It is also

[1] DeCew, In Pursuit of Privacy: Law, Ethics, and the Rise of Technology, 73 (1997).

necessary to have a private place in order to have any kind of concept or opinion. Additionally, seclusion enhances social interaction on a variety of ways. According to Daniel J. Solove, a society without privacy is a "suffocating civilization."[2] It's also worth noting that scientific advancements played a key part in the creation 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 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. 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.

[2] *Ibid.*

1.2 Statement of problem

There are many debates in recent times on the topic relating to privacy of individual in todays rapidly developing world and the Indian legislations relating to privacy. The public is in doubt about their privacy rights , and they strongly hold and opinion privacy is not only violated by the commercial sector but also by the government at large in many forms. General public has a notion that no one will protect their privacy. The public expressed strong favour for enlarging the ambit of people's legal rights to stop anyone without authority to peep into their personal data . But however privacy is not a small talk of the town rather it is very complicated to derive legislations that actually solves all the problems relating to privacy. In todays time privacy is considered as constitutional Right and even Fundamental Right and it needs to be protected. With the increasing population of technology it has become crucial to frame some suitable legislation on privacy.

1.3 Aim

The researcher by this dissertation seeks to define privacy elaborately and make an in depth study to various facets of right to privacy. While doing so, the researcher will go into the various socio, legal, and ethical aspects of right to privacy. The researcher will also touch some international aspect with special emphasis on India. The researcher will also investigate the judgments of the Supreme Court of India on the subject.

1.4 Research Objectives

- To study about how right to privacy evolved over time.
- To study the awareness of privacy among people
- To study usages of excessive surveillance techniques both by public and private agencies.
- To study unregulated uses of technologies having potential to invade individual's privacy.
- To study the tussle between freedom of media and rights regarding privacy.
- To study the role of websites for social networking in present information society.

- To study role of judiciary in recognising different facets to right to privacy in India.

1.5 Literature review

An article under the tile of "Invasion of privacy" whose author is annicka Gunnarsson said that in this world full of technology Privacy is a crucial privilege that must be safeguarded. People must be in power of the knowledge about themselves and they alone should decide which information has to be stayed inside their home and what to be go outside in the world. Sadly, this power of keeping privacy is under attack these days that should be protected. There are many solutions existed for this but we have to fight this together. Major threats caused to our privacy is due to increasing free market and capitalism. The main reason for violation of privacy in a capitalistic society is the focus of everyone on earning money. Some other reasons are technology and increased usage of electronic information. Now a days our personal information is stored in databases and those databases can be a threat to breach of privacy. The misuse of our personal information kept in various databases is the main subject of this research.

Another article under the name of "right to privacy and freedom of press- conflicts and challenges " whose author is Gifty totally deals on an unique aspects and talks about how a n information can be taken by devices for recording or taking of pictures and later uses those records according to their usage by changing and modifying them is an serious violation of privacy by the press. The cause of worry is that availability of any information becomes so easy and at the same time securing privacy becomes difficult due to continued upgradation in technologies. There is no specific legislation or any mechanism to book the journalist and seek any remedy for the breach of privacy. The information by press spread with great speed without anyone caring about the authenticity of the information. They just keep spreading it among the public and within 2 minutes it is shown to million of people around the world. This paper tries to depict how easy it be to put the privacy of any person at stake by the media for their own benefit.

The article titled "Informational privacy: legal introspection in India," according to the paper. Written by Payal, it examines the growth of privacy rights in depth, as evidenced by a number of Supreme Court decisions. As a result of this work, the judiciary has

recently recognised privacy as a legal right in both the private and public domains, and the right to privacy has been recognised as a basic right.

The article titled “Right to privacy in digitalized India” authored by Santhosh S Discusses in detail the emergence of privacy in India as a concept and its impact on the overall Indian economy. This document focuses on the privacy rights of digital India and its impact on Indian citizens, especially considering that many people live in highly technologically isolated areas where it is difficult to receive telephone signals, not to mention connecting to the Internet using modern facilities such as online banking, etc. Therefore, it is worth noting that the impact of privacy rights can be open to everyone in a country, which inevitably leads to different situations. With the emergence of the Aadhar card, it is also crucial to note that the biometric data of each citizen of India is stored in a huge database, which will create countless security problems, which will come from countless potential cyber threats. These are all potential threats, and are actually an assessment of whether Indian citizens will enforce their rights.

Article titled “A review of big data security and privacy issues” authored by mahamadou kante extensively deals with the latest developments that took place in cyberspace. Social media has led to the data explosion because users are seen sharing data from every corners of the world. Thus, the big data opportunities come with the challenge of security. Big data's success depends on a thorough awareness and management of rapidly growing vulnerabilities. This paper examined the most recent research and development on the most pressing security and privacy challenges in the Big Data industry. The qualities and value of big data are discussed first. Then he goes over various security and privacy concerns and issues, and then he makes some recommendations for further research.

Article titled ”What is privacy: the history and definition of privacy” authored by Adrienn Lukacs Makes a brief discussion about the importance of privacy, which is closely related to human dignity, freedom and individual independence. It is increasingly being questioned in the information society's period of rapid technological growth. The goal of this study is to highlight an impression of the history of secrecy in order to better comprehend the idea and propose methods for properly protecting privacy in the digital age. Existing definitions, then international legal norms, especially

how the European legal norms regulate privacy protection, and finally the current issues of the information society.

The article titled ”On privacy and security on social media” authored by Senthil kumar Shows how social media has become a part of human life. Starting from sharing texts, photos, news and other information, many people began to share the latest news and pictures about media news, issues, training tasks and seminars, online surveys, marketing and customer concerns. Business and jokes, music and video in entertainment. In fact, because Internet surfers use it in various ways, we call social media today’s Internet culture. Like to share on social media, but it takes a lot to ensure safety and privacy. User information that cannot be disclosed must be kept confidential. This document aims to emphasize privacy and security measures related to social media.

1.6 Research Questions

- How far the people have awareness of RTP.
- How far the practice of surveillance methods both by public and private agencies is justified.
- Whether unregulated use of technologies have potential to invade individual’s privacy.
- What is the role of media in violating the RTP of people and how to prevent those violations?
- How far the websites for social networking having data of individuals have potential to invade in right to privacy of individuals.
- What is the role of Indian judiciary in recognising the different facets of right to privacy in public interest.

1.7 Research Methodology

The researcher has adopted the doctrinal method of study for the completion of this paper. This study has been designed keeping in view the research objectives and to address the research questions effectively. In order to do so, the researcher bring in use both the primary and secondary sources of data to take the study towards a sound and logical conclusion while giving recommendations, if any, for the same. The researcher

will go through various statutes, books of both Indian and foreign authors, articles, journals and periodical reports by the competent authorities.

1.8 Research Design

Chapter 1

Introduction

Chapter 2

It defines the concept's definition, nature, and extent of RTP. The Chapter starts with philosophical discussions of eminent philosophers like Aristotle, John Locke, J.S. Mill, Samuel Warren and Louis Brandeis. It will also cover the awareness of privacy among people and how surveillance techniques impact the people's right to privacy.

Chapter 3

It includes the Constitutional provisions protecting right to privacy in India.

Chapter 4

In today's technology age, this Chapter concentrates on the security of an individual's personal information. Individual personal data has become an essential 'raw material' for innumerable government and corporate entities, as well as critical products, services, performances, and obligations. The privacy challenges of today's information era have been examined in this chapter.

Chapter 5

It will address the conflict between media freedom and individual privacy rights, investigative journalism and privacy issues, making public private facts, the legal framework for media, and the interpretation of press freedom.

Chapter 6

It deals with role of judiciary in making fundamental right to privacy and how Indian judiciary has evolved the law related to right to privacy with its various judgements.

Chapter 7

Conclusion and suggestions

Chapter 2

MEANING, NATURE, SCOPE OF RIGHT TO PRIVACY AND CONCEPT OF SUEVEILLANCE

2.1 Introduction

‘Privacy’ varies from time to time, society to society, culture to culture, and community to community. Irrespective to the variation in its extent, each section of our society gives value to such sacred concept. Many writers also noticed the roots of the concept of ‘Privacy’ in the past well-known philosophical discussions. For example, Aristotle’s differentiation of public and private sphere in a city-state is one of the earliest philosophical discussions. In the state of nature, as John Locke said, nobody had exclusive rights to the earth and other natural resources. People had common control over the property. Each person, on the other hand, had a right to his or her own identity as well as the right to self-preservation. Furthermore, by performing labour, an individual might create his own private property, distinct from the common property.

John Stuart's Work titled as 'Liberty' provides for the best difference between the private and public in philosophical literature. He has talked about his most famous principle which is known as 'Harm Principle'. This principle clearly states that it is only justified to use power upon any member of the civilised society with force only if such act will protect every other member of society from greater harm. Through this theory he draws the attention towards a phenomena where the activity of one individual has a deep impact over the life of others and in such cases government can enter into the matter to save a larger population from probable harm, mainly those area's of activities that are openly subject to public supervision. Public sphere is different from private sphere with the fact that, it affects huge population and society but in the case of private sphere only individual who performs the activity gets affected or few others who voluntarily subject themselves. state or public intervention is unreasonable in private sphere of the Individual, so this area of action is legally inaccessible to the public, and in this sense

is private. J.S. Mill said that the individual is sovereign over himself, over his own body and mind.[3]

Furthermore, with the publication of the article 'Right to Privacy' in Harvard Law Review in 1890, legal discussion on the idea of 'Privacy' began. The authors of the article were Samuel Warren and Louis Brandeis. They really initiated a debate in the legal field, which culminated into the constitutional recognition to the 'right to privacy' in 1965.[4]

Indeed, Ferdinand Schoeman observed: "*Despite the fact that privacy has been identified by contemporary philosophers as key aspect of human dignity, or alternatively as something even more basic than rights to property or than rights over one's own person, there was no major philosophical discussion of the value of privacy until the late 1960s".*[5]

In the words of Samuel D. Warren: "*Solitude and privacy have become more essential to the individual, but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress".*

Louis D. Brandeis remarked: "*The protection afforded to the thoughts, sentiments, and emotions expressed through the medium of writing or of the arts, so far as it consists in preventing publication, is merely an instance of the enforcement of the more general right of the individual to be let alone".*

Therefore, almost all of the philosophers are agreed on the universal value of the concept of 'Privacy. However, they have the divergent viewpoints regarding the definition of 'Privacy'. It has also been said that because individuals' personal outlook and their experience of encounter with privacy is poles apart due to difference in socio-historical contexts, So it becomes extremely tough to define the concept of privacy and even more challenging to measure.[6]

[3] J.S. Mill, On Liberty. 13 (1967).
[4] Griswold v. Connecticut, 381 U.S. 47 (1965).
[5] Ferdinand Schoeman, "Privacy: Philosophical dimensions." in Ferdinand Schoeman (ed.), Philosophical Dimensions of Privacy: An Anthology, 1-33, at 1 (1984).
[6] Debbie V. S. Kasper, "The Evolution (or Devolution) of Privacy" Sociological Forum, Vol. 20, No. 1: 69-92

2.2 Perspectives on the Meaning and Value of the Term "Privacy"

2.2.1 “Privacy” and Human Dignity

“Samuel Warren” and “Louis Brandeis” wrote:

“The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury”.[7]

According to “Warren” and “Brandeis” privacy refers to keeping a control on third party access over the individuals private data. The underlying goal of his article is to call attention to the invasion of privacy that occurs when personal data is published or disseminated without the users' agreement.

The author points out that recent inventions and commercial practices have prompted society to take steps to guard personal identity and ensure the “right to be let alone”. They also raised a concern about the abuse of technical quality by a photography and newspaper company that has attacked the sacred corners of private and family life and transcended etiquette.

Warren and Brandeis advocated that legal recognition should be extended to RTP in order to be well protected. Including property, copyright, contract and trust tort law used to protect privacy in the past, the law should clearly allow individuals to govern the level of their opinions, feelings, reactions, and works, regardless of whether they are commercial or artistic value that can be used in public domain and known to world. The transition to a clear law aims to emphasize that the law recognizes people’s moral and spiritual integrity and their material interests.

[7] Samuel D. Warren and Louis D. Brandeis, “The Right to Privacy," Harvard Law Review, Vol. 4, No. 5 (Dec. 15, 1890). pp. 193-220, at 196. Available at http://www.jstor.org stable/7321160

2.2.2 Privacy and Control over Information

It is believed that the concept of 'privacy' has been narrowly construed by some authors who focus mainly on control over information about oneself. And such narrow views which were protected by Warren and Brandeis and by William Prosser are also recognized by more recent observers including Charles Fried and William Parent. "Alan F. Westin defines Privacy" as *"The claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others"*.[8]

William Parent gives several reasons for valuing 'privacy'. Firstly, if someone manages to obtain sensitive personal knowledge about an individual, he acquires power over the individual. Such power could be misused against the individual. William Parent believes that there is the clear link between the harmful impact and invasion of privacy and that could be one of the major possibility as to why individuals don't want their private unrecorded data to go into public domain. when people in society lead an unbearable lifestyle that is very distinct from the normal pattern and approach of society , the desire for privacy increases manifold. When the Habits and ways of thinking of an individual is completely different from majority in Society, their weaknesses become objects of contempt and ridicule. No one wants to be a laughing stock and being embarrassed. Moreover there are many private stuffs in a person's life that should not be passed to a stranger or into the public domain.[9]

Parents' views on personal data not only consider some data breaches, but also include some situations that don't seem to be violation of privacy at all. If A notices in a public meeting that B is too sensitive to his height and uses a shoe lifter, and A strongly draws a opinion that B is short. After this A has gathered some unofficial personal knowledge of B, but A is obviously not peeping into B privacy. A somehow thought a conversation discovered that B is an alcoholic person but however this information is unofficial in nature. After this A gathered a bit of information that was

[8] *Id.,* at 7.
[9] *Id.,* at 276.

undocumented personal information. This case shows that A has not at all invaded the privacy Of B.[10]

2.2.3 Privacy and Interpersonal Relationships

A lot of authors believe that having privacy is crucial for maintaining important relationships with intimate areas of life. Intimacy is impossible without respect for privacy. Although Charles Fried values the concept of privacy, he developed his own paper and stated that privacy must be linked to goals. And the most basic relationship: respect, love, friendship and trust. In addition, he believes that such a basic relationship (love, friendship and trust) is simply unimaginable if privacy is not recognized. The basic relationship requires a the presence of privacy. Therefore, attacks on privacy inevitably endanger our personal integrity.[11]Charles Fried said :

Respect, love, trust, a sense of connection with others, and seeing us as the object of love, faith and warmth are the core of our self-image as individuals in the crowd, and privacy is crucial environment for this attitude to develop and for our actions to take place. Privacy is as important as oxygen for combustion.[12]

According to Charles Fried, "*Privacy, is control over knowledge about oneself. But it is not simply control over the quantity of information abroad; there are modulations in the quality of the knowledge as well. An individual may not mind that a person knows a general fact about him, and yet feel his privacy invaded if somebody knows the details. Fried cites an example, i.e. there is no violation of privacy where a casual acquaintance may comfortably know about the sickness of an individual, but it would violate the individual's privacy if another person knew the nature of his illness"*.[13]

[10] James H. Moor. "The Ethics of Privacy Protection," Library Trends, Vol. 39, Nos. 1 and 2, Summer/Fall 1990, 69-82, at 76. Available at https://www.ideals.illinois.edu/bitstream/handle/2142/7714/librarytrendsv39il2h_opt.pdf?sequence= 1
[11] Charles Fried. "Privacy." The Yale Law Journal, Vol. 77, No. 3 (Jan., 1968), 475-493 at 477, available at http://www.jstor.org/stable/79494
[12] *Id.,* at 478.
[13] *Id.,* at 483.

2.2.4 Privacy and Restricted Access

Several theorists describe privacy in terms of admittance. Sissela Bok, which is counted as one of the notable philosophers, defines privacy as a state of protection that prevents unnecessary access by others, whether it is physical access, personal information, or concerns. Ruth Gavison gave his view which even extended the ambit of this argument. According to Ruth the essence of privacy lies in the fact that how much accessible it is to the world. According to him The limited availability principle of the concept of privacy allows us to determine when a loss of privacy takes place. For Gavison, the far crucial term is loss of privacy. They stress that privacy can be achieved in three different and self-governing but interwoven ways and they are : Solitude, Secrecy and anonymity. Furthermore, the reasons for our demands for privacy in many situations are similar, and they are all related to the purpose of privacy in our lives: supporting freedom, autonomy, individuality, and interpersonal connections, as well as creating a free society."[14]

According to Anita Allen, "*Personal privacy is a condition of inaccessibility of the person, his or her mental states, or information about the person to the senses or surveillance devices of other"*.[15] Given this definition, privacy is a descriptive, neutral concept. Isolation, separateness, confidentiality, discretion, and obscurity are systems of privacy. It is being believed that Allen knows about the problems raised by the term accessibility: it is ambiguous, nearly synonymous with 'privacy,' and applicable in different respects at the same time. Allen views the latter as a virtue of her theory and argues that restricted-access privacy is more illuminating than accounts that focus on command over material about oneself (Reiman), control over access or attention to oneself (Gavison), and intimacy (Gerety). In defense of her definition, Allen cites the practical link between privacy, and restrictions on access that protect it, and a common usage of the term 'privacy' denoting conditions of limited access. Her broader argument is that liberal principles of personhood, involvement of all citizens as equals, and maximum contribution in accordance with one's abilities necessitate privacy.

[14] *Id.,* at 423
[15] Anita Allen, Uneasy Access: Privacy for Women in a Free Society, 15 (1988).

Privacy helps children create and maintain autonomy by allowing them to choose whether or not their physical and psychological existence becomes a part of another person's experience. To regard yourself as self-determined, you must have this level of control. This claim is supported by research on both identity development and degeneration. Psychologists like “Jean Piaget and Victor Tausk” believe that a child's developing sense of self is dependent on her ability to control information about herself. She considers herself to have some control over what occurs to her.[16]

2.2.5 Scope of Privacy

In one of the most well-known cases, Griswold v. Connecticut, the United States Supreme Court issued a judgement in which privacy was recognised as a constitutional right. Regardless of informational privacy or the "Fourth Amendment of the United States Constitution," this constitutional right to privacy is recognised. Simultaneously, the court permits married couples to utilise contraception. The right to constitutional privacy, according to Judge William O. Douglas, protects privacy areas such as the social system of marriage and married people's sexual relationships. Constitutional privacy not only protects the right to use and spread contraceptives, but also protects abortion rights and future funding decisions, fathers' rights, third-party consent to minors, and fetes protection. Privacy has been used to allow "possession of obscene matter" at home. Related to sterilization laws, multi-racial marriages, and attending public schools. The concept of privacy is also seen revolving in the cases related to marriages, attendance at public school etc.

Inspite of the court ruling to safeguard personal matters of Individuals , Coherentists (those who has a thinking that privacy is a coherent concept) did not agree on this issue that is When constitutional privacy and constitutional data protection cases involve personal lifestyle and family choices, they include freedom of birth control, multi-racial marriage, watching pornography at home, and abortion. By saying that constitutional privacy cases only focus on freedom and liberty, William Parent explicitly excluded concerns about the ability of individuals to make choices about their family and lifestyle as a real privacy issue. Others holding this view are Henkin, Thomson, Garvison and Bok.

[16] Joseph kupfer, “Privacy, Autonomy. and Self-Concept." American Philosophical Quarterly, Vol. 24, No. 1 (Jan., 1987), 81-89 at 82, available at http://www.jstor.org/stable/20014176

In the famous case of “whalen V. Roe” The United States Supreme Court affirmed the view that privacy consists of two aspects: controlling personal information and controlling your power to make certain key decisions. As per the court RTP means that an individual is interested in maintaining secrecy about personal affairs and is also interested in making certain important decisions.

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.

Control over personal data, as well as our bodies and personal decisions about ourselves, is facilitated by privacy. Privacy, according to some authors, is a jumbled concept that includes I controlling information about oneself, (ii) controlling one's interests related to physical and mental well-being, and (iii) controlling one's ability to make important family and lifestyle decisions, express oneself, and develop diverse relationships. These three interests are linked because risks exist in each of the three environments: dangers to information leakage, threats to our ability to govern our bodies, and challenges to our ability to make our own judgments about our own lives and activities make us vulnerable to doubt, pressure, or use by others. Faced with so much attention, pressure and exploitation It also agreed that privacy is important because it protects personal information, natural space and personal choice, as well as freedom and autonomy in a free democratic society. Ferdinand Schumann eloquently advocates the importance of privacy to protect self-expression and social freedom.

It is widely understood that privacy helps citizens in exercising moral autonomy, which is a crucial requirement for governing democracy. The literature shows that privacy not only has internal and external value to , but also has an impact on the social roles and relationships of relevant personnel. Privacy rules aid in the organisation of social connections such as romantic, familial, and professional ties, such as those between physicians and patients, lawyers and clients, teachers and students, and so on. Secrecy can improve social interaction at all levels. In the words of Solove “ *A society without privacy is a Suffocating society”*.[17]

[17] Daniel J. Solove, Understanding Privacy, (2008). Quoted in DeCew, Judith, "Privacy” , The Stanford Encyclopedia of Philosophy (Fall 2013 Edition), Edward N. Zalta (ed.), available at http://plato.stanford.edu/archives/faU2013/entries/privacy/

Even Indian Judiciary have begun to interpret privacy rights more widely. The most important development relating to personal autonomy took place in the famous case of Naz Foundation V. NCT Delhi decision which is extended by Delhi High Court. After reviewing the case law of data protection in India, the Delhi High Court focused on the RTP, which has been upheld to guard a person's personal space where one can become and follow one's own personal autonomy.[18]

As a result, the Supreme Court's current strategy is to safeguard individual privacy. By giving more and more personal autonomy to the individual, the Supreme Court is also protecting his decisional privacy. In fact in S. Khusboo v. Kanniammal also, the court recognized the Live-in relationship which is again a right of decisional privacy. The rigid attitude of the courts against the practices of honour-killings is an another step towards the protection of one's right to choose his or life partner.[19]

In Suchita Srivastava and Another v. Chandigarh Administration, The Supreme Court ruled that according to Article 21 of the Indian Constitution, a woman's right to choose whether or not to have a child falls under the heading of "personal liberty." The court decided that no limits on a woman's reproductive choices should be imposed, based on her right to privacy, dignity, and physical integrity., such as women's right to refuse sexual intercourse or sexual activity or her choice to Stick to contraceptive methods.

Articles 19(1)(a) and 19(l)(g) of the Indian Constitution, which deal with freedom of speech and expression and freedom of trade, profession, and other activities, respectively, provide a home for an individual's personal autonomy. While legalising dances at bars, hotels, and other establishments, the Hon'ble Supreme Court has recognised the dancing ladies' personal liberty over their choices and decisions in State of Maharashtra v. Indian Hotel & Restaurants Association.

Therefore, it is submitted that the trend is now to expand the concept of privacy. By giving more and more personal autonomy, the State protects individuals' privacy rights.

2.3 Concept of surveillance

Surveillance is, without a doubt, a key tool for social control. However, the current extent of monitoring has grown significantly, and it now extends far beyond suspects,

[18] Cited in Graham Greenleaf, "Promises and illusions of data protection in Indian law" , International Data Privacy Law Vol.l.No.l: 47-69 at 49
[19] Bhagwan Dass v. State (NCT of Delhi), (2011) 6 SCC 396.

criminal activity, and national security concerns. Eventually, every person is under surveillance. For example, surveillance over children, educational institutions watch students, employers spy on employees, surveillance by religious leaders, police surveillance, and government agencies watch peoples' behaviour and so on. It is also being observed that the 'surveillance' is inevitable to tackle the crime, which has been increased due to development in science and expertise.[20]

Alan F. Westin divided surveillance into three categories to explain it: physical surveillance, psychological surveillance, and data surveillance. These sorts of surveillance, on the other hand, are not new to any culture. Eavesdropping and paid surveillance agents have been used since times immemorial. Torture, sex, alcohol, opium, hypnotism, primitive "lie" tests, and tests for proper "personality" are also ancient ways of unlocking minds, extracting information, or implanting suggestions. As for data surveillance, ancient societies used to maintain registers in which residences, movements, and transactions of individuals were recorded. Every collection of records helped the society in mechanism of administrative social control.[21] The researcher observed that in the contemporary society, all private and public agencies have huge amount of information regarding individuals' personal details. Such personal details are being misused for many purposes. So far as the government agencies are concerned, it has been seen that they are misusing it for political purposes.

Whenever, the term 'surveillance' comes into our mind, nightmares of Big Brother society start vibrating our thoughts. Basically, the phrase 'Big Brother is Watching You!' was used in the novel named '1984', written by George Orwell published in the year 1949. In this Chapter, the phrase "Big Brother is Watching You!" has been used as a metaphor. The novel depicts a totalitarian society in which the government has complete surveillance over the people. Big Brother (fictional name given to the government) is supreme ruler and continuously watching people through telescreens (giant sized televisions), which have been installed in peoples' homes, streets, markets, or any other private or public places. In the novel, it has been depicted that the government manipulates every public document because the Big Brother does not want people be informed of reality. Brain washing propaganda feels people as if they are living in an idealist state. Moreover, the Telescreens, which have been installed at

[20] Alan F. Westin, Privacy and Freedom, 57 (1970).
[21] *Id.,* at 68.

homes, are capable of recording sounds, images, and facial expressions of individuals. Additionally, the Telescreens transmit such material back to the police named, 'Thought Police'. Then, the novel says that the Thought Police could easily decipher an individual's state of mind by using the recordings of one's movement, reflexes, and facial expression. By doing so, the police find out what kind of thought a person is possessed with. If thought is against the conservative ideology of Big Brother, then it will be considered as 'Thought Crime'. Increasingly, police helicopters frequently snoop in peoples' windows and finally, punish 'thought-criminals'. Therefore, there is no escape from Big Brother's camera.

In ancient India, Chanakya' s Arthasastra describes that Maurya empire used to deploy spies and secret agents, as tools of military strategies. Internal espionage and inspection, the emperor's hard work and attentiveness, and a skeletal monetary economy with cash payments were the foundations of loyal and efficient bureaucracy in the days of difficult communication. The king's efficiency to control the administration was usually relied upon the pool of information created by able sleuths. Similarly, Mughal system, despite its weaknesses, was considered as powerful, flexible, and intricate in terms of surveillance system. During British India, the integration of surveillance systems that had previously been independent and supposed to keep check on each other resulted in the creation of new and arbitrary centres of authority. Use of professional spies and official snooper were common in British India.[22] By conducting surveys in India, British enhanced their control on villages, and collected territorial revenue at large scale. Village, subdivision, and district boundaries were established. This was a part of the declaration of sovereignty. British controlled and generated information for conquest, trade, and administration in India by deploying indigenous surveillance and intelligence networks.

As a result, any society is familiar with the government's monitoring practises. The fundamental difference between historic and modern monitoring measures, however, is technical innovation. With the increase in the science and technology, the government's monitoring ability has become more powerful. Today, it has become very easy to conduct surveillance. By using new sophisticated technologies, everybody is able to capture another's image, videos or recordings very easily and, to store them

[22] C. A. Bayly, "Knowing the Country: Empire and Information in India" , Modern Asian Studies, Vol. 27, No. 1, 3- 43, at 6, (Feb., 1993).

permanently. And it can be done even without the subject's knowledge. In the past, physical activity monitoring was based on observations with the naked eye and simple equipment such as binoculars. Now it can be done through night vision cameras and thermal imaging cameras, complex magnification and telescopic equipment, tracking tools, and transparent sensor technology. Most of the transaction records of hospitals, banks, shops, schools, and other institutions could only be found in file cabinets before the 1980s. Now, with the arrival of computers and the Internet, they are easier to obtain.[23] Moreover, it has also been observed that the use of privacy destroying technologies is on rise since 9/11 attacks in United States and 26/11 attacks in Mumbai. Definitely, people justify government's surveillance power in the panic conditions of terrorism. People do believe in the government's programmes of collecting personal details. People have trust in the government that their personal details will be protected against an unauthorized access. Video surveillance, location monitoring, data mining, heat detectors, spy satellites, and X-ray scanners have changed the state into a state of Argus in this period. Government is seen keeping a tracks about the People's personal life which consists of monitoring about their daily activities, taste, preferences, likes , dislikes etc. so large-scale surveillance breaks the balance between privacy, information disclosure, and surveillance.[24]

At the same time, the impact of surveillance on human behavior cannot be ignored. Excessive surveillance involves serious repercussions. In the situation, where subject knows that he is under continuous surveillance, he would either accept social norms or violate them. But compulsion to reveal those parts of his memory and personality that he regards as private, amounts to violation of person's psychological privacy.[25] 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:

"On the outside, the individual can hold objects of self-feeling such as his body, his immediate actions, his thoughts, and some of his possessions clear of contact with alien

[23] Christopher Slobogin, Privacy at Risk, 3
[24] Daniel J. Solove, Nothing to Hide, 2
[25] *Supra* note 32 at 58.

and contaminating things. But in total institutions these territories of the self are violated".[26]

Individuals' freedom of association, right to talk freely, right to communicate anonymously, and other rights are increasingly being harmed by the government's vast gathering of personal information. It can be happened in a case where the government does not want to be criticized by its dissenters. For political purposes, government may misuse individuals' personal information.

However, in all this discussion it has been observed by many authors that the concept of 'surveillance' found no distinct place in sociological lexicon until 1970s. David Lyon observed that even James Rule's ground-breaking study of Private Lives and Public Surveillance, which was appeared in the early 1970s, could not attract social theorists' attention. Rather it was Michel Foucault's studies of surveillance and discipline after which social theorists began to take 'surveillance' seriously. Surveillance, according to Anthony Giddens and others, should not be viewed as a reflex of capitalism (watching factory workers) or the nation-state (keeping administrative tabs on citizens), but as a source of power in and of itself. It is apt to mention here the reference of some more sociological studies on surveillance. The Marxian and Weberian works on surveillance is of utmost importance. Karl Marx Considers worker surveillance as a technique of sustaining capital's management control.

"Michel Foucault" was a French historian and philosopher who lived from 1926 to 1984. He influenced a varied range of humanistic and social scientific areas, not just (or even largely) in philosophy.[27] In his book Discipline and Punish published in 1975, Michel Foucault used the term 'Panopticon'. Basically, Panopticon was an imaginary machine designed in 1791 by Jeremy Bentham, a British architect and legal reformer. Even though monitors do not see each inmate all the time, but they could see inmates at any time from the central tower. In such architecture, the inmates always act as if they are under continuous observation. Prisoners' awareness of their complete visibility would self regulate themselves. For Foucault, This guarantees that power functions

[26] Erving Goffman, Asylums, 23 (1961). Quoted in Joseph Kupfer, "Privacy, Autonomy, and Self-Concept," American Philosophical Quarterly, Vol. 24, No. I (Jan., 1987), pp. 81-89 at 83. Available at http://www.jstor.org/stable/200N176

[27] Gutting, Gary, "Michel Foucault", The Stanford Encyclopedia of Philosophy (2012) available at http://plalo.stanford.edu/entries/foucaidt

automatically since prisoners internalise it without the need for an external enforcer to be there at all times.[28]

However, today's ubiquitous surveillance system has executed the functions of prisoners' Panoptican model in the whole society. Everyone is subject to the Closed Circuit Television ("CCTV") cameras monitoring. Individuals know that they are being watched, thus, they do behave themselves. Furthermore, individuals could never see the enforcers e.g. camera control operators or monitors. Foucault argued that *"spread of the idea of 'Panoptican' , in the society, makes the governments more powerful. It is so because of the fact that people internalize the surveillance and behave in ways that conform to the requirements of power. In such process, people are constructed as subjects or objects for whom information is collected and collated. The individuals' personal information is utilized as per according to the requirements of power"*.[29]

Therefore, modern communication technology has made the surveillance system, a Superpanopticon model which does not require any tower or guards. Sophisticated surveillance devices and databases of individuals' information have automatically disciplined the population. Moreover, individuals' every transaction, either voluntarily or compulsorily, with public and private agencies proves that population is participating in its own self-constitution as subjects of the normalizing gaze of the Super panoptican. In this whole participation, people don't even know that they are under State's continuous surveillance and control.[30]

Therefore, it can be said that the government's surveillance- physical, psychological, and data surveillance- may use the techniques of Biopower "for achieving the subjugations of bodies and the control of populations".

Furthermore, it was observed by Zigmund Bauman that discipline is not necessary for producing a docile labour force because such labour force is available everywhere in the present globalized world. He argued that televised broadcasts of celebrities have made the whole mechanism a seduction. The Panoptican has been replaced with a new technique of power named as 'Synopticon'. The term 'Synopticon' was coined by Thomas Mathiesen, was of the opinion that the mass media has shown a new power

[28] Eugenia Siapera, Understanding New Media, 108
[29] *Ibid.*
[30] Mark Poster, The Mode of Information, 97 (1990).

tactic in which people are turned into spectators. .Bauman's argument here is that this technique of power, which is implemented by the mass media on the one hand, gives the image of transparency and equivalence between the observed elites and the viewers, thus legitimising the current condition of inequality. In order to achieve conformity, it stifles any dissenting voices by propagating a set lifestyle to be copied and praised. Similarly, for David Lyon the fact that the many watch the few legitimizes and justifies that the jo few can watch the many.[31]

Generally, it is believed that sophisticated devices or other privacy destroying technologies are being used by government or law enforcement agencies only. But widespread use of such technologies in private sector has also raised the alarm for privacy advocates. It is so because of the fact that unregulated use of privacy-destroying technologies involves very serious privacy issues.

Moreover, the public and private bodies have also added Biometric technologies in their surveillance scheme.

A biometric system is a pattern recognition system that determines the validity of a user's physiological or behavioural attribute in order to make a personal identification. It is, in fact, a type of physical measurement. Facial recognition techniques, fingerprints, hand geometry, voice, iris, retina, vein patterns, palm print, Deoxyribonucleic Acid (DNA) samples, and other biometric technologies are examples. However, there are many privacy issues which are inherently attached with the biometric technology. Because biometric data cannot be withdrawn, there are concerns regarding its security in a variety of domains. If biometric data gets compromised, an individual could face significant problems. If an individual's biometric data gets substituted by malicious data, then the innocent individual could be treated with suspicious eyes. It has been suggested that a biometric safety arrangement should be based on the concept of "authentication without identification," with the identification of the individual and the type of access he should have as the first step.

2.4 Electronic Surveillance Technology

In order to protect their own interests, every public and private authority is relied on the modern surveillance technologies. Obviously, widespread electronic surveillance

[31] Eugenia Siapera, Understanding New Media, 109

violates individuals' privacy rights. It has also been seen that due to technological innovations, today's surveillance can be done without even touching a person's physical body. People hardly know about their surveillance. Due to the difficulty of detecting surveillance technologies, a subject under monitoring may discover that chats, emails, and activities that were considered to be private communications or acts were really seen and tracked.[32]

"Electronic surveillance" can be done through the installation of Closed Circuit Television ("CCTV") cameras, wiretapping, "bugging," pen-register, global positioning system (GPS), and the electronic interception of e-mail.

2.4.1 Cameras and Facial Recognition Technique

Individuals' behaviour patterns and value systems are inevitably being influenced by increased surveillance. When a person is not trusted, he tends to retaliate by being untrustworthy himself. And the individual who is being observed, whether electronically or otherwise, unknowingly becomes more cautious in what he does and says.[33]

In such conditions, a person won't be able to develop his ideas and thoughts. It is quite possible that his whole mind will be conditioned automatically as per according to the requirements of the society. Therefore, it can be said that the restriction on an person's autonomy affects his psychological privacy.

The Closed Circuit Television ("CCTV") cameras have been installed almost everywhere in the society like villages, schools, hospitals, creche, 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.[34] 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. Many rights will be jeopardised, including the right to be different, the right to hope for tolerant forgiveness or overlooking of previous foolishness, errors, humiliations, or minor sins (notion of redemption), and the right to start over. The usage of facial

[32] Vance Packard, The Naked Society, 11 (1964).
[33] A. Michael Froomkin, "The Death of Privacy?," Stanford Law Review, Vol. 52, No. 5, 1461-1543 at 1477, (May, 2000).
[34] A. Michael Froomkin, "The Death of Privacy?," Stanford Law Review, Vol. 52, No. 5, 1461-1543 at 1477, (May, 2000).

recognition technology is another recent component of closed-circuit television (CCTV) monitoring. Facial recognition software can recognise a person's face in a variety of photos or video recordings. By installing “Mandrake” system, the London police matched Closed Circuit Television (“CCTV”) Photos of known criminals were compared to photos collected from shopping malls, parking lots, and train stations. Simultaneously, it is feasible to develop a gadget that will alert a person whenever a person convicted of rape, child molestation, murder, or theft approaches within 100 feet. It would undoubtedly be a violation of the prohibition against double jeopardy.

However, the facial recognition technology still needs improvement, as it lacks perfection. If it falsely alarms the law enforcement agencies to suspect an innocent individual, it would cause embarrassment and humiliation to the individual. Furthermore, if the facial recognition system fails to catch a real culprit, one would hardly expect it a fair and efficient surveillance device.

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 compulsory to sustain a record 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 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 person’s rational belief of secrecy.

There was incidence of leakage of the Delhi metro train Closed Circuit Television (“CCTV”) footage has narrated the story of the unregulated use of Closed-Circuit Television (“CCTV”) camera recordings. It was reported that Closed Circuit Television (“CCTV”) Couples' intimate moments were captured using cameras installed in Delhi Metro trains. Furthermore, the video material was recorded and uploaded to pornographic websites. It was also alleged that 13 videos had been published to porn sites, with approximately 1.5 lakh individuals watching them. Many such videos are thought to have been made but have yet to be released into the public realm.

2.4.2 Wiretapping or Phone Tapping

When the matter of law is involved officials use a lot of techniques such as those of phone Tapping either to collect the evidence or to know the entire truth. Wiretap is a tool through which government can do almost everything with the individual phone call such as listening, recording etc. A tap also performs similar functions that of wiretap but the only potential difference is that it user web signals to operate rather then wire.[35]

However, the government is required to show more justifiable reasons to get interception order than in case of search warrant, as phone tapping or wiretapping has strong potentiality to intrude into a person's privacy. For interception order, the government must inform the court about the nature of the offence, location and device to be intercepted, reasons or factors showing inefficiency of alternative methods, and the total period of interception. However, in United States, the legislation named "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)," has diluted the above said pre-requisite conditions for communications interception. Law enforcement agencies, such as the Federal Bureau of Investigation, have had their powers expanded as a result of the act. In the current world, the government has gathered an endless number of law enforcement instruments, notably in the fields of surveillance and the internet. The USA PATRIOT Act of 2001 (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001) gives the FBI and other government agencies full access to personal information kept by service providers. The law enforcement agency does not need a court order for this. The authorities can demand the users' details from the service providers with a mere statement certifying that the information is necessary for the investigation. Therefore, the law enforcement agencies can conduct wiretap of any telephone number, computer, and mobile on the ground of mere suspicion of a crime. Such process of wiretapping at large scale is known as 'roving wiretap'. Furthermore, the authorities can conduct secret wiretaps for the foreign intelligence purpose.[36]

In India, Section 5(2) of the Telegraph Act 1885 states that the Central Government, State Governments, or any officer specially authorised in this regard can intercept

[35] Andrea L. Johnson, "Wiretapping", in William G. Staples (ed.), Encyclopedia of Privacy, 609-612 at 609

[36] *Id.,* at 611.

communication messages in the event of a public emergency or in the interest of public safety if satisfied that doing so is necessary or expedient in the interest of India's sovereignty and integrity. On the other hand, Rule 419A of the Indian Telegraph Rules 1951 provides a procedural safeguard against phone tapping. This rule was amended in 2007 to curb the misuses. At present, only the Union and State Home Secretaries are authorized to order for interception of messages.

Because phone tapping is such a serious violation of an person's secrecy, the government should only have the authority to intercept communication communications. If it is allowed to any private body or individual, it would be dangerous attack on people's freedom. Such apprehension could be manifested through the unregulated use of mobile phones, smart phone, or any other gadgets in the present techno world. It has been observed that people are hardly sensitized towards each other's privacy rights. Obviously, it may spread a sense of insecurity among people in the society. People may start losing trust in each other. In Rayala M. Bhuvaneswari v. Nagaphanender Rayala, the husband pleaded that he should be allowed to produce a hard disc, in which he recorded his wife's telephonic conversations surreptitiously. But the court said that the tapes cannot be admissible in evidence because the husband's action was illegal as well as a violation of wife's privacy.

Indeed, the lawful interception can only be done by the public authorities. However, lawful interceptions are subject to the judicial review. The constitutional legitimacy of the Maharashtra Control of Organized Crime Act, 1999 (MCOCA Act) was challenged in the case of State of Maharashtra v. Bharat Shanti Lai Shah. It was argued that the State legislature lacked the authority to pass such law, and that the Maharashtra Control of Organized Crime Act, 1999 (MCOCA Act) is unconstitutional and violates Article 14 of the Indian Constitution. The Supreme Court, on the other hand, maintained the Act's constitutional legitimacy, stating that the Act's goal of preventing organised crime authorises the State legislature to create such legislation and intercept communications. In addition, the court determined that the Act has enough procedural safeguards, meeting the criteria of Article 21 of the Indian Constitution. The Supreme Court ruled in this case, based on its previous rulings, that the right to privacy may be limited in conformity with legal procedures that are just, fair, and reasonable.

Late. Arun Jaitley, the then opposition leader in the Rajya Sabha, alleged that the government tapped his phone for political purposes. However, Union Home Minister Sushil Kumar Shinde has disputed that BJP leader Arun Jaitley's phone was tapped, claiming that the issue involved private individuals illegally getting the Rajya Sabha Leader of Opposition's phone contact records. He said that it is not a matter of phone tapping rather illegal access to Call Data Record (CDR). He said the illegal access will be probed thoroughly. Similarly, in Himachal Pradesh, the Congress government turned over the phone tapping case to the State Vigilance and Anti-Corruption Bureau (SV&ACB) for further inquiry to determine who was responsible for the illegal phone tapping.[37]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.

The advent of private sector players in telephone industry is making the situation worse. The Telegraphic Act of the 18th Century is ill-equipped to meet the upcoming challenges. The rules framed under TRAI Act, 1997 regulate the present functioning of Telecom companies including the private sector. Telecom Unsolicited Commercial Communications by Telecom companies invading personal privacy of consumers.[38]

2.5 Psychological Surveillance

Psychological surveillance refers to scientific and technological approaches used to gather information from a person that he does not want to reveal, does not realise he is revealing, or is forced to reveal without a mature understanding of the implications for his privacy. [39]

The Polygraph test, also known as Tie detection' test, was developed as an instrument to aid police in the detection of crime. The theory behind the polygraph is that lying causes distinctive and measurable physiological reactions in a person who knows that he is not telling the truth. The polygraph operator asks questions in a special pattern while testing the subject's heart and pulse rate, relative blood pressure, breathing, and perspiration rate. Bodily changes are recorded by pens on graph paper, producing

[37] "Himachal: Phone tapping case handed over to vigilance bureau,"Available at http://articles.timesofindia.indiatimes.com/2013-04-07/india/38346018_1_previons-bjp-regime-vigilance-officialsvigilance-bureau

[38] G.R. Lekshmi, "Electronic Surveillance- A tool of invasion of privacy" , The Academy Law Review, Vol. 32: 1&2: 223-256 at 231

[39] *Supra* note 32 at 133

"squiggles" resembling those on an electrocardiogram or seismograph. By interpreting these records, a trained polygrapher is supposed to be able to identify untrue responses to critical questions.[40]

Personality tests are increasingly being used to identify personality traits for the aim of appraising an individual's psychological strength, particularly to predict future performance in a role such as employment. In addition to emotions, attitudes, propensities, and level of personal adjustment, personality tests also measure subject's attitude towards sexual, political, religious, and family matters. Both polygraphing and personality testing raise the question of whether employers or the government should be able to force people to have their inner processes examined by machine or test assessments.

Moreover, there are other relations of voyeurism to the problem of surveillance. It was observed by many researchers that polygraph operators do ask embarrassing personal questions to female subjects. It satisfies their erotic desires. Similarly, during wiretapping the authorized officials record the intimate conversation and play it to their friends just for entertainment.

2.6 Data Surveillance

Historically, every government is in the habit of collecting personal details of individuals for having control over them. In that sense, the process of collecting the personal information of individuals is a part of surveillance system'. According to Roger Clarke:[41]

Indeed, Roger Clarke also mentioned the dangers of Data Surveillance. In case of personal Dataveillance, an individual could face dangers like wrong identification, data flows without his knowledge or consent, blacklisting, his denial of redemption etc. Similarly, in case of Mass Dataveillance, an individual could be denied the due process clause, and climate of suspicion can be spilled over to the whole society.. As Clarke mentioned, other dangers to society include adversarial relationships, law enforcement focusing on easily detectable and provable offences, inequitable application of the law, decreased respect for the law and law enforcers, decreased self-reliance and self-

[40] *Ibid.*

[41] Roger Clarke, 'information Technology and Dataveillance," Communications of the ACM, 31(5): 498-512. Available at http://www.rogerclarke.com/DV/CACM88.html

determination, a weakening of society's moral fibre and cohesion, and the potential for repressive measures.[42]

One of the earliest mode of gathering information by the government is the Census. The census provides much information to the policy makers. Therefore, it is very necessary for the people to participate in the surveys conducted by the government. However, with the passage of time, the governments increased the questions in the questionnaires. These questions sought more personal information about people. Furthermore, governments gather and retain an endless amount of records, such as a person's name, date of birth, place of birth, name and ages of parents, voting records, home address, telephone number, property details, police records such as arrest records, court records, and so on. By doing so, the governments make the personal dossiers of every individual. And it is paradox that people hardly know about the existence and content of such dossiers.

Earlier, only the government was interested in collecting the personal data of social and economic importance. But since the early 1990s, private sector has vastly been engaged in such transactional data systems. Sophisticated strategists in the industries like consumer credit, direct marketing, insurance, and publishing, enhanced profit by tailoring the consumers' personal data.[43]

In the cyber age, everybody inevitably leaves trails of his personal information and hence, such personal data provides the infinite opportunities to organizations to make calculated appeals to specific individual for commercial transactions. Therefore, commercially motivated organizations exhaust every resource for Target Marketing and Target-Pricing. In Target-Pricing, sellers adjust their prices by watching the consumers' previous purchase history.

Moreover, telephone companies and Internet Service Providers do have the personal details of its subscribers. Whenever the individual downloads any software, calls anyone, sends or receives e-mail, upload videos, etc., the Internet Service Providers

[42] *Ibid.*

[43] James B. Rule, "Towards Strong Privacy: Values, Markets, Mechanisms, And Institutions" , 54 University of Toronto Law Journal, 183-225 at 195.

may make dossiers of such transactions.[44] Similarly, social networking sites do possess the personal information of its users, which is being used for multi-purposes.

The government also taps the personal data possessed by libraries. An individual's library details can reflect his personality as well as ideas or thoughts he's possessed with. Similarly, law enforcement authorities use patterns of behaviour, purchases, and hobbies to evaluate person's future conduct.[45]

2.6.1 Census Survey and Aadhaar Card System in India

First of all it is crucial to understand about the concept of census survey. If defined in the simplest term, it refers to collecting data from the general public about a lot of things related to their life such as about their purchase , income, families etc. After collection of data they are compiled and those compiled data is analysed to drive out conducive results.

The oldest literature, the 'Rig Veda,' suggests that a population count was kept about 800-600 BC. The Arthasastra of Kautilya, written circa 321-296 BC, emphasised census taking as a gauge of state policy for taxation purposes.[46]

Even at the time of the Mugal period when Akbar was on thrown, census was conducted for purpose of taxation. [47]

In British India, however, survey activities are viewed as a scientific "panoptican," designed to give colonisers with a comprehensive network of monitoring and control over the Indian countryside and population. Furthermore, penitentiary authorities were supposed to furnish the police with details of released convicts in order to give the forces of the law the opportunity to substitute for jail and to carry on reform work. The released convicts had to register their names in the habitual-offenders' register. Despite increase in surveillance, crime was not being tackled. The police thus started a vast enterprise in each district of writing deviant world down, subdividing the population meticulously into identities, castes, addresses, habits, offences, condemnations. Among

[44] Jerry Kang, "Information Privacy in Cyberspace Transactions'; 50 Stan. L. Rev., 1193-1294 at 1233, (1998).
[45] Daniel J. Solove, "The Future of Privacy" , American Libraries, Vol. 39, No. 8: 56-59 at 57, (Sep., 2008).
[46] http://censasindia.20v.in/Ad Campaign/drop in articles/05-Histow of Census in India.pdf
[47] *Ibid.*

these categories, caste was vital. A social cartography of criminal castes was established so as to isolate groups 'scientifically' and indicate the dangerous groups.[48]

The Registrar General of Citizen Registration is responsible for creating and maintaining the National Register of Indian Citizens, as per the Citizenship (Registration of Citizens and Issue of National Identity Cards) Rules, 2003. The National Population Register (NPR) is a comprehensive identity database that will be overseen by the Registrar General and Census Commissioner of the Ministry of Home Affairs. During the 2011 House Listing and Housing Census phase, data from all typical inhabitants was collected for the National Population Register. The National Population Register will contain three categories of data: demographic, biometric, and Aadhaar data (Unique Identity Number). Demographic data includes information such as a person's name, father's name, mother's name, sex, date of birth, current and permanent home address, relationship status, relationship to the head of family, place of birth, occupation, nationality, and education. Biometric data includes photograph, fingerprints and iris prints. Thereafter, list of local register of usual residents (LRUR) will be displayed in the local area. Such list will contain demographic data and photograph. After scrutiny and authentication of local register by local registrars, data collected in National Population Register.[49]

Furthermore, Raytheon, an American defence company, said It was in talks with the Indian government to lend its expertise in putting up the Rsl,200-crore National Intelligence Grid (NATGRID) project, which will allow law enforcement agencies to share information more effectively to combat terrorism both at home and abroad. Raytheon India President William L Blair said, "What we have done in United States National Counter-Terrorism Centre might be relevant to India's National Intelligence Grid (NATGRID). One of Raytheon's biggest customers is United States (US) government. They know our strength. We are ready to offer our technology to India in this area."The corporation would give India with the most modern technology available," it was agreed. The National Intelligence Grid (NATGRID) will have access to a number of databases, including those pertaining to train and air travel, income tax, bank account information, credit card transactions, visa and immigration records, land

[48] Arnaud Sauli, "Circulation and Authority" , in Claude Markovits et. al. (Eds.), Society and Circulation, 215-239 at 229.
[49] "E-Governance Initiatives-Changing Lives for the better," Press Information Bureau, available at http://pib.nic.in/newsite/erelease.aspx?relid=69324.

records, internet logs, phone records, gun records, driving licences, property records, and insurance.[50]

The researcher argues that the cumulative effects of national population register along with unique identity number, National Intelligence grid (NATGRID) and recent Information Technology Amendment Act 2008, have the potential to make India an Argus State. Under the name of security of state, the government is now planning to perform mass surveillance of an entire population.

"However, it has been claimed by the authorities that the personal information will be protected and kept confidential. The government can use such information within its various agencies. Under the National Identification Authority of India Bill 2010, it has been provided that the authorities will protect identity information and authentication records of individuals. Similarly, aadhaar number holder can access and alter demographic and biometric information in his record. The authority shall not disclose such information to any person. But information will have to be disclosed in pursuance to court's order or in the interests of national security to the appropriate authority. It has been provided that unauthorized access will be punished."

2.6.2 Data Interception under Information Technology Act

Despite numerous forms of cyberspace privacy violations, the government conducts surveillance via electronic communications and data kept on a server. The recently updated Content Technology (Amendment) Act of 2008 broadened the scope of providing orders to monitor any information on the internet. In the year 2019, the central government issued the Interception Rules 2009. They were enacted under section 69 of the Act, and they defined how to protect information interception, monitoring, and decryption (the "Interception Rules 2009").[51]

Under section 69B, the government can also monitor and collect traffic statistics or information generated, transferred, received, or stored in any computer resource. Information that can be used to identify and locate any human, computer system, or computer network is referred to as "traffic data." The Central Government has issued

[50] "Raytheon in talks with Indian government over NATGRID project," PTI, Daily News and Analysis. available at http://www.dnaindia.com/india/1557930/report-raytheon-in-talks-with-indian government-over-natgrid-project.
[51] http://cis-india.org/internet-governance/blog/privacy/safeguards-for-electronic-privacy.

the “Monitoring and Collecting Traffic Data Rules, 2009” to carry out this monitoring. Thus, the draconian regime of surveillance has increased the threats to individuals’ privacy.

The reasons for the interception must, however, be documented in writing. The competent authority shall examine alternate methods of obtaining necessary information before issuing the intercepting orders. The commands must include specific information from a specific computer resource.

The “Information Technology Act” mandates that any subscriber, intermediary, or person in control of a computer resource provide all types of information, facilities, and technical support to law enforcement agencies in order to improve data surveillance. The assistance is to:

- Provide access to the computer resource comprising material; or
- Intercept, monitor, or decrypt the information; or
- Provide stored information

2.6.3 Access to and Censorship on Social Networking Sites

Anupam Chander examines two opposing perspectives on the Internet's role in authoritarian regimes. The first point of view is upbeat, in which he considers Habermas' idea of citizens' participation in public debate. It emphasizes on the fact that people’s participation, in the making of public policies, is the basic edifice for every democratic set up. And because of the social networking sites, such public participation has been increased. Social networking sites enable person’s to say straight to their nationals and to the nation. It has been seen that the internet helped dissidents to circulate information in unfree societies. The tragic video of Neda Agha-Solten, who was murdered as she protested against Iranian repercussion, was smuggled out of the country and finally, uploaded at social networking sites like Facebook, YouTube, etc. The video really shocked the conscience of the world. Similarly, Burmese citizens used Google’s Blogger and YouTube to reveal government’s suppression in the year of 2007.[52]

[52] 4 Anupam Chander, “Googling Freedom,” California Law Review, Vol. 99, No. 1: 1-46 at 2.

However, repressive states are shutting down the internet and social networking sites to stop people’s protest. Alternatively, the repressive states can make the social networking sites as their auxiliaries, and in return, the social networking sites may get the free access to the local market. Anupam Chander uses Foucault theory to understand the issue, and sees the internet as a facilitator of the surveillance state. In such a case, the digital network itself might make political dissidents vulnerable, providing the secret police with a veritable black book of names and addresses. It was also uncovered that by partnering with China and other authoritarian governments, Google, Microsoft, and Yahoo betrayed the people of China and other authoritarian countries. However, social networking companies are obligated to preserve people's fundamental rights, particularly in authoritarian nations.

Chapter 3

CONSTITUTIONAL PROVISIONS AND LEGISLATIVE MEASURES REGARDING RIGHT TO PRIVACY IN INDIA

3.1 Constitutional Provisions Recognizing Right to Privacy in India

The ancient evolution of the concept of 'privacy' brought the contention that courts and commentators are actually protecting the sense of dignity that is at the core of any privacy idea.[53] Moreover, the researcher also observed that the International instruments and conventions have also played significant role in recognizing the right to privacy. And it happened only because of the recognition given to the human rights, which were derived their existence from the inherent dignity of human beings.

Furthermore, the researcher argues that it is the accountability of the State to create such a social milieu in which every individual could live with human dignity. Ronald Dworkin believes that the government should treat everyone equally with care and respect. Individuals have inherent dignity and moral worth, independent of who they are or where they stand, which the state must not simply recognise passively, but actively care about. For this, the Constitution of the State should provide the basic human rights to its citizens so that they could enjoy their dignified life.[54]

The Indian Constitution's Preamble stipulates that:[55]

"WE, THE PEOPLE OF INDIA, having solemnly resolved to constitute

India into a [SOVEREIGN SOCIALIST SECULAR DEMOCRATIC

REPUBLIC] and to secure to all its citizens:

JUSTICE, social, economic and political;

LIBERTY of thought, expression, belief, faith and worship;

---

[53] Jeremy M. Miller, "Dignity as a new Framework, Replacing the Right to Privacy" , in Thomas Jefferson Law Review, 30:1 (2007), 1-52, at 50. Available at http://ssrn.com/abstract= 1 127986

[54] Rhoda E. Howard and Jack Donnelly, "Human Dignity, Human Rights, and Political Regimes". The American Political Science Review Vol. 80, No. 3: 801-817 at 803, (Sep., 1986).

[55] The Constitution of India, 1950, The Preamble. Available at http://indiacode.nic.in/coiweh/coifiles preamble.html

EQUALITY of status and of opportunity;

and to promote among them all FRATERNITY assuring the dignity of the individual and the [unity and integrity of the Nation];

IN OUR CONSTITUENT ASSEMBLY this twenty-sixth day of November, 1949, do HEREBY ADOPT, ENACT AND GIVE TO OURSELVES THIS CONSTITUTION".

Every individual's dignity is guaranteed in the Indian Constitution's Preamble. It also ensures that all Indian persons have admittance to righteousness, liberty, and equality of position and opportunity. The Preamble recognises individuals' personal autonomy and self-respect by guaranteeing their freedom of thinking, expression, religion, faith, and worship. An individual realises his inner and exterior visions of life in this type of environment. Similarly, administering justice, equity, and good conscience is being considered as a pre-condition for executing the idea of human dignity.

While administering justice, everybody should be treated equally. However, 'right of equality' is not a mathematical formula. With a view to provide dignified life to all persons, the idea of 'positive discrimination' has been preserved under Articles 14, 15 and 16 of the Indian Constitution. Again, these provisions seek government's active efforts for bringing fairness in equality. At the same time, it is pertinent to mention that the term "dignity" is very wider in scope, and could only be achieved when the government fulfils the individuals' basic necessities like food, clothing, shelter, education, etc.

Article 17 endeavours to abolish the barbarian practice of untouchability. Everybody in the society possesses the same level of dignity and self-respect. Nobody wants that he or she should be treated as if he or she is an alien to the society. Such type of discrimination unnecessarily exposes one's private life to the society. In consequence of this, the individual may be segregated and stigmatized. He or she may be branded with stigmatized words. He or she would feel ashamed and embarrassed if people start behaving indifferently with them.

Natural justice values, such as justice, equity, and fairness, are recognised in Article 14 of the Indian Constitution. When human rights and fundamental freedoms are infringed, Article 14's justice principles come in and restrict all government acts. In fact, the judiciary frequently employs these concepts in evaluating arbitrary and discretionary

powers. The Indian Supreme Court has ruled that administrative entities must always act in accordance with the "fairness" principle. Even, while enacting any legislation, the Parliament cannot forget the principles of natural justice. The combined effect of Articles 14, 19 and 21 proclaims that the government cannot take away individuals' rights. If it does so, then it becomes necessary for them to adopt just, fair and reasonable procedure. Recently, lesbian and gays' rights were also recognized on the basis of Article 14. An illogic and unreasonable action of the government which abridges away lesbians' and gays' rights, is an intrusion into one's decisional privacy.[56]

In general, 'freedom of speech and expression' is seen as the polar opposite of 'right to privacy.' However, freedom of speech and expression includes the right to talk freely and anonymously, which is a part of the "right to privacy."[57] Increasingly, such privacy version covers the arguments protecting the speech and expression of Whistle-blowers. Indeed, the Whistle-blowers' Protection Bill, 2011, enacted by the Lok Sabha, aims to offer proper protection to those who disclose corruption or deliberate misuse of discretion that results in demonstrable loss to the government or the commission of a criminal offence by a public official.

Article 21 of the Indian Constitution recognises RTP as a Fundamental Right. The central government is empowered to legislate on the subject of privacy and data protection by utilising the powers conferred under Article 246(1). Parliament is vested with enough power to enact on matters of List I ,seventh schedule.

Indian domestic laws are strictly separated from international laws. It means that any of international treaty will not become the part of Indian law until it has been incorporated into the Indian law by the Parliament itself. The Indian Parliament, under Article 253 of the Constitution, has the authority to enact any law necessary to carry out any foreign treaty or convention.

While reiterating its earlier observations on international treaties, the Supreme Court in "Sheela Barse v. Secretary, Children' s Aid Society", for the first time recognized the binding character of the international treaties and conventions. The court said that India, being party to the International Charters, is under an obligation to implement the international treaties and agreements in the proper way. The Supreme Court in Vishaka

[56] Naz Foundation v. Government of ACT of Delhi, 2010 Cri. LJ 94 (Del.).
[57] Daniel J. Solove, The Digital Person, 177

v. State of Rajasthan reminded the Indian government of the provisions of the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW) 1981, and stated that in the absence of domestic legislation, international conventions and norms should be read in conjunction with the fundamental rights enumerated in Part III of the Indian Constitution. The court also developed guidelines for preventing sexual harassment and other forms of abuse against women at work.

3.2 Various Legislations for the Protection of RTP in India

As the researcher observed that although there is no specific and direct law on right to privacy, various legislation and constitutional provisions do recognize and protect individuals' privacy rights in India.

3.2.1 Efforts to Recognize Right to Privacy under Indian Penal Code, 1860

Every person is born with a sense of self-protection. He has an inherent right to protect his physical body from any kind of assault. In order to protect physical privacy, the Indian Penal Code prescribes certain provisions i.e. Section 96 to Section 106, regarding Right of Private Defence. This right is not confined only to protect one's own human body but also any other person's body. In fact, historical idea of protecting possession of property is also covered under the right of private defence. In certain circumstances like murder, rape, unnatural offence, kidnapping, abduction, etc., the right of private defence allows an individual to take away the life of the attacker. Privacy rights in one's property are further authenticated u/s 27 of IPC. It is provided person's possession continues even if the possession of property lies with his wife, clerk or servant.

The Indian Penal Code protects individuals from being maliciously prosecuted. Similarly, it also punishes those public servants who act contrary to law and cause injury to a person. Injury includes both physical and psychological. Similarly, if any person knowingly gives false information to public servant, who causes injury to another person, he (who gave false information) will be punished for such action. For giving same kind of protection to one's self respect and psychological peace, the law punishes those persons who knowingly either institute false criminal proceedings against another person or charge him on false grounds. It is submitted that these provisions are very helpful in protecting an individual's reputation, self respect, autonomy, and many other privacy rights.

Similarly, in order to protect the victims of crime from being stigmatized, criminologists and penologists have concentrated their thoughts on the study of Victimology. The study focuses on the rehabilitation of victims of crime. The first step of rehabilitation is cemented on the fact of non-disclosure of the identity of victims of crime. Therefore, S. 228A of IPC, 1860 punishes every action of publication which discloses the identity of rape victims.

Every person has right to enjoy his or her personal moments in peaceful, hygiene and healthy environment. 'Public Nuisance' does affect the privacy rights of people in the form of causing injury, danger or annoyance to the public.

The researcher submits that religion is a very personal matter for every human being. Everybody has right to worship one's own God. He or she can practice their religious ceremonies. Therefore, if anyone insults another's religious feelings, it amounts to violation of his religious privacy. Indeed, section 295 punishes a person who intentionally or knowingly insults another's religion by way of damaging or destroying any place of worship or any other sacred object. Similarly, section 295A punishes those who outrage one's religious feelings.

It is submitted that Life is meaningless without 'personal liberty'. Even Indian Constitution provides liberty to move through territory of India to every citizen. It also recognizes personal liberty to every person. Thus, if anyone unlawfully or illegally restrains or confines one's lawful movement. The Indian Penal Code punishes both wrongful restraint as well as wrongful confinement.

The Code protects female's privacy in S.354 of the IPC protects the modesty of a woman. Furthermore, if someone assaults or uses criminal force with the intention to dishonor a person, he is subject to the punishment. Similarly, section 509 punishes anyone who says something, makes a gesture, shows something, or intrudes on a woman's seclusion with the goal to offend her modesty.

Right to Privacy is, generally, considered as very close to the concept of slander and libel. The reason being this is that in both circumstances one's reputation is at stake. Thus, Indian Penal Code punishes the act of defaming others and hence, protects their reputation.

"An offence of defamation under Section 499 Indian Penal Code, 1860, requires three basic ingredients which are as follows:

I. Making or publishing any imputation concerning any person.
II. Such imputation must have been made by words either spoken or intended to be read or by signs or by visible representations
III. The said imputation must have been made with the intention to harm or with knowledge or having reason to believe that it will harm the reputation of the person concerned.

Therefore, an intention to cause harm is a pre-requisite condition for an offence of defamation. An offence punishable under Section 500 Indian Penal Code, 1860 requires blameworthy mind and is not a statutory offence requiring no mens rea."

3.2.2 Provisions respecting Privacy under Code of Criminal Procedure and Indian Evidence Act

If the investigator believes that the production of a particular document or item is necessary or crucial to the investigation, he can issue a written order to the person who possesses or authorises the document or item to suspect the production of the document or item under Article 91 of the Criminal Procedure Law. According to Article 91 of the Criminal Procedure Law, the court may also order the above-mentioned documents or things to be provided.

If the documents or items required for the investigation are likely to be in one place, and the investigator has reason to believe that these documents or items cannot be obtained immediately by other means, the assigned officer can give reasons for the conviction after written notice. , Provide written documents or measures to be taken to conduct house or apartment searches in accordance with Article 165 of the Criminal Procedure Law. If possible, the registration is carried out by the same official, but if he cannot conduct the search in person, he can ask his subordinate officials to provide written reasons. A written order to conduct a search; the designated order must specify the place of registration and, where possible, the items or documents that will be searched. A copy of the results of a search under Article 165 (1) or (3) shall be sent immediately to the next judge or special judge who has the authority to prosecute the crime.

3.2.3 Procedural Safeguards under certain legislations like “The Narcotic Drugs and Psychotropic Substances Act, 1985 and Income Tax Act, 1995”

“The Drugs and Psychotropic Substances Act of 1985” takes drug crimes very seriously and provides for severe penalties. In order to balance "power of search " and "privacy rights", the law also provides certain procedural guarantees. This Act provides for the right to search in the presence of an official or a magistrate. The search official must explain to him that he has the right to be searched in the presence of the official or judge, and whether the person wishes to be registered with the official or magistrate. Judge, he must be Bring it to a civil servant or judge and register; however, if the assigned officer belives that he cannot be brought to a Gazetted officer or judge without giving him the opportunity to give up drugs, controlled substances , etc., he can treat him or her according to Article 100 of the law. some cases, a search can be conducted without a court order (by a judge) or permission. (By an official). When conducting such a search, the officer must provide his supervisor with a copy of the written information or reason for the conviction within 72 hours.

Servey refers to thorough inspection, or more generally, conducting research. The purpose of the survey is to identify, collect, review and compare information to arrest tax evaders. The survacy is generally a sudden inspection by income tax officials to check relevant information, check the balance on the account book, check the location of the stock and the location of the stock on the account book, etc. Section 133A of the Income Tax Law begins with the words *“ Notwithstanding anything contained in any other provision of this Act”.* Therefore, these regulations are independent and do not include other regulations of the IT Act.

Therefore, S.133A of the IT Act deals with powers of survey. It stipulates that the tax authority can enter any place within its jurisdiction or where people under its jurisdiction conduct business or occupations, and requires the person in charge to assist in checking the accounting books and provide all relevant information. They can even inspect the cash, supplies, or other valuables kept therein, however the income tax authorities can only access any business or professional premises during the authorised location's open collecting hours. After sunrise and before nightfall, look for alternative locations.

Keeping books or papers for more than 10 days, on the other hand, requires the chief commissioner's or chief executive officer's consent. The authority can count all cash holdings, inventories or other items or values that it has inspected or verified. A statement by a person who may participate in a lawsuit under the Income Tax Law. However, the testimony during the interrogation does not have much evidential value compared with the testimony during the search. In addition, the tax authority can inquire relevant information about the expenses incurred, Appraisers related to functions, ceremonies or events. The purpose of the investigation is to collect useful information about tax evasion control. Therefore, the investigation does not require the victim to be notified in advance. The information obtained from the survey can be used to supplement the assessment.

Another tool for uncovering tax avoidance is search. A thorough check of the "building, place, vessel, vehicle, or aircraft" is referred to as a search. S.132 of the IT Act.

The search warrant must be duly filled out, signed and sealed by the competent authority in the prescribed form. The name of the person who issued the permit must be included on the permit and cannot be left blank with the registration authority. There were cases in the past where an empty warrant was issued. Signing such a search warrant will make the search illegal. In addition, it violates the purpose of procedural safeguards guaranteed by law. The legality of the search warrant can be challenged in the competent court.

3.2.4 Telecom Regulatory Authority of India

Telecom has become an integrated part of our society as almost each and every member of the society is directly or indirectly associated with it. 'Telecommunication Service' is a wide term that includes electronic mail, voice mail, data services, cellular mobile telephone services.[58] In such wide ambit of services, it is evident that the consumer using these services may have grievance from time to time regarding quality of service, increase in service charge, disconnection of services etc. As a result, the Telecom Regulatory Authority of India (TRAI) was founded in 1997 under the Telecom Regulatory Authority of India Act, with the purpose of creating an effective regulatory framework with sufficient protections to encourage fair competition and consumer

[58] Vikas Asawat, "Consumer and Telecommunication Service: Role of Telecom Regulatory Authority of India in Policy making and Regulations" , available at http://ssrn.com/abstract= 1873525

protection. The government has been expanding the Act's scope to include television and cable services since January 2004. The Telecom Regulatory Authority of India (TRAI) issues tariff guidelines for basic telephone, cellular services, Direct to Home (DTH) services, and other services from time to time, and one of the TRAI's primary tasks is to regulate price fixing. All telecom operators are required to keep the Telecom Regulatory Authority of India (TRAI) informed about their tariff schemes as they are implemented in compliance with TRAI standards.[59]

The Telecom Regulatory Authority of India (TRAI) has taken a great move in the interest of consumers by implementing Mobile Number Portability (MNP), which allows mobile phone subscribers to switch operators without changing their numbers. This will give independence to customer to change the service providers if they are not satisfied with their service. Prior to MNP, customer was not able to change the operator as his existing mobile number was key contact information to many people and by changing the number he may lose his business etc.[60]

Uninvited Marketable Communications have been a chief source of annoyance and disruption for telecom consumers in current years. Individuals' privacy is invaded by these exchanges. Telecommunications is increasingly being utilised to advertise and market various products as the country's telecom services develop and telecom costs decline. On the 5th of June, 2007, the Telecom Regulatory Authority of India (TRAI) published the Telecom Unsolicited Commercial Communications Regulations, 2007 to regulate unsolicited commercial communications. It proposed the establishment of a National Do Not Call (NDNC) Registry to enable registering requests from customers who do not want to receive UCC easier.

The Telecom Regulatory Authority of India (TRAI) agreed to build up a National Do Not Call (NDNC) Registry Portal to enforce the abovementioned legislation. The Telecom Regulatory Authority of India (TRAI) then enacted the "Telecom Commercial Communications Customer Preference Regulations, 2010," which govern several elements of telecoms service providing to customers. For example, Do Not Call Registry, partially blocked category, restriction to unsolicited commercial

[59] *Ibid.*
[60] *Ibid.*

communications, regulations on standards for quality of service, and guideline on a code of practice for metering and billing precision etc.[61]

The Telecom Regulatory Authority of India (TRAI) Act, 1997 was changed in January 2000, and the Telecom Disputes Settlement and Appellate Tribunal (TDSAT) was established, with both original and appellate jurisdictions. It is a special tribunal established solely to resolve disputes between the Department of Telecommunications (DoT) and a licensee, or among two or more facility providers, or between a service provider and a group of clients, among other things..[62]

3.2.5 Indian Copyright Act, 1957

Intellectual property rights is also one of the privacy right which gives an autonomy and control over one's own ideas, knowledge, literary works, photographs, etc. Meanwhile, increase in technology has enhanced the threat of piracy in every artistic work. Availability of copyright material on the internet and its theft by way of hacking has further demoralized the authors Databases are protected in this way because they are collections or compilations of literary and artistic works. Databases are protected as "literary compositions" under the Indian Copyright Act, which includes, among other things, computer programmes, tables and compilations, and computer databases (The Copyright Act, 1994). The author's talent, labour, and judgement are all protected, regardless of how the output appears..[63]

The "Indian Copyright Act, 1957", covers "Databases" as "literary works" u/s 13(1) (a), which states that "Copyright shall exist throughout India in original literary, dramatic, musical, and artistic works." Computer programmes, tables, and compilations, including computer data bases, are included in the definition of literary works under Section 2(o) of the Copyright Act, 1957". According to S. 63B of the Indian Copyright Act, anyone who knowingly uses an unauthorised copy of a computer programme on a computer will be sentenced to a least of six months and a extreme of three years in prison.

---

[61] See Telecom Commercial Communications Customer Preference Regulations, available at http://www.nccptrai.gov.in/nccpregistjy/regidationl diccndiv.pdf
[62] Telecom Regulatory Authority of India (Amendment Act), 2000, s. 14.
[63] Alok Kumar, "Copyright in Digital Era" , available at http://www.rmlnlu. ac. in/web/alok_kumar_yadav.pdf

In India, the Copyright Law protects computer software's Intellectual Property Rights (IPR). As a result, the provisions of the Indian Copyright Act 1957 safeguard computer software copyright. In and of themselves, the June 1994 revisions to the Copyright Act were a watershed moment in India's copyright landscape. The Copyright Law made it apparent for the first time in India:

- A copyright holder's legal rights.
- Rental software position
- The user's ability to produce backup copies

The Copyright Act was necessary since most software is easy to reproduce and the copy is usually as good as the original. The following are some of the most important components of the law:

- It is illegal to manufacture or distribute copies of copyrighted software without valid or particular authorization, according to Section 14 of this Act.
- The offender can be prosecuted both civilly and criminally.
- Injunctions, actual damages (including the violator's profits), or statutory damages per infringement may be sought in civil and criminal actions.
- Violations of software copyright can result in harsh penalties and fines.

3.2.6 The Indian Contract Act, 1872

Another option for data protection is the Indian Contract Act. Both the federal and state governments can create the "contracts" described in Appendix III. The Indian Contract Act of 1872 must be followed by state legislation. According to the law, if one party breaches a contract, the other party is entitled to compensation for the loss or harm suffered. So the major concern of contract Act here is that those companies who are acting as " data exporter" should enter into a standard form of contract with those companies to whom they are supplying data ,in order to secure highest degree to data authenticity. Since these contracts have binding nature , it can be even used on international platform. Moreover as the business is growing around the world it is seen that parties have started inserting arbitration clauses to the contract.

3.2.7 Specific Relief Act, 1963

In addition to the compensation, an aggrieved party can specifically enforce his right or claim, if accrued in the violation of right to privacy. In India, the Specific Relief Act 1963 provides for the specific enforcement of certain rights. Another noteworthy feature of this legislation is the provision of preventive remedies in the form of temporary and permanent injunctions under sections 37 and 38, respectively. The complainant can take the injunctions orders from the court to prevent any breach of contract, obligation, etc. Under injunction orders, the court can restraint any person from doing certain things which are prejudicing the interest of the plaintiff. Similarly, the court can also direct any person to do some act for bringing the balance of convenience among the parties. If any service provider does not fulfill his contractual obligation, the plaintiff can plead for injunction orders in the court of law. Such remedy is effective in various privacy issues like trespass, nuisance, defamation, easementary rights, etc. In addition, under section 40, a plaintiff seeking an injunction may seek damages in addition to or instead of the injunction.

3.3 The Indian Telegraph Act

It was the "Indian Telegraph Act 1885" that governs the wiretapping. The S. 5 of the Act clearly talks about that authority is empowered to intercept messages if that are related to public good.

Article 7 (2) (b) empowers the government to impose rules outlining the safeguards to be taken to avoid improper communication interception or disclosure. However, in the case of People's Union for Civil Liberties v. Union of India, it was discovered that the government had not issued any such guidelines or rules. However, when it comes to wiretapping by the government, the Supreme Court of India has issued the following guidelines:

- A tap order is authorized to be issued by only high chaired persons such as Union Home secretary or his counterpart.
- The government has the obligation to prove that this is the last way left to gather vital information.

- Government is also entrusted with the responsibility to setup a standard committee to review the legal aspects of every wiretap.

Despite the existence of these laws, it is agreed that due to problems in their implementation, they do not provide adequate protection, and that privacy laws will only be effective when the relevant citizens take into account their rights.[64]

3.4 The Privacy (Protection) Bill, 2013

The Privacy (Protection) Bill of 2013 aims to provide privacy to each and every users in cyberspace and their personal information from the government, government agencies, individuals, commercial organizations, etc. It also aims at addressing the conditions under which individuals are monitored which is infringing their privacy rights. So overall this Bill focuses its attention on securing rights of individuals in every possible way.

Following are some features of the Bill:

- Every power under this Act shall be exercised by following some privacy principles namely, *"(a) that personal data belongs solely to the person to whom it pertains; (b) that personal data is required by governments and commercial service providers and others to enable public safety, good governance and the delivery of services without undue delay; (c) that the right to privacy is recognised as a fundamental human right by various international treaties to which India is a party; (d) that intrusions into privacy need always be measured by necessity and tempered by proportionality; (e) that the right to privacy is essential to the maintenance of a democratic society; (f) that the right to privacy cannot override the right to information; (g) that privacy must be upheld by a competent authority that is independent, impartial, well resourced and free from unwarranted influence".*[65]
- RTP has been recognized to all persons.

[64] Delia S. Tantuieo, "Online Privacy and Confidentiality: Legal Issues in Cyberspace" , Media Asia, Vol. 29 No. 4: 193- 196, at 196

[65] The Privacy (Protection) Bill, 2013, s. 3. Available at http://cis-india.org/internet-governance/blog/privacyprotection-bill-2013.pdf

- The Bill's requirements will not apply to the collecting of personal data for personal or family use, or the surveillance of a resident's residential property.
- Personal data shall be collected for limited purpose only. Before collecting any personal data, the person's informed consent should have been taken. Moreover, the person seeking information should inform the concerned person about the whole mechanism of data processing i.e. the manner, purpose, transfer, retention period, safeguards, etc. of his personal information.
- Personal data must not be kept for longer than is required to fulfil the purpose for which it was obtained. However, with the approval of the person concerned, any personal data may be maintained for a longer amount of time, or the data may be required to be stored for historical, statistical, or research purposes under the requirements of an Act of Parliament.
- Section 9(2) provides, "Any person who collects, receives, stores, processes or otherwise handles any personal data of another person shall be subject to a duty of confidentiality and secrecy in respect of it." Similarly, section 10 prohibits disclosure of personal data to any other person. However, disclosure can be done by taking the informed consent of the person. However, in this scenario as well, a person wanting to disclose personal information is required to inform the individual concerned about the entire data processing mechanism, including the name and address of the person to whom the personal data will be transferred. It would keep one's sensitive information safe from third parties. However, the consent is not required in cases where the disclosure is compulsory i.e. access to law enforcement agencies for preventing, investigating or prosecuting a cognisable offence.
- Sensitive personal information shall not be reserved for unreasonable time. It shall be processed for limited purpose only. Sensitive personal information shall not be disclosed to any person except the person to whom information pertains.
- No individual can intercept any communication of another individual without the order by the Chief Privacy Commissioner. Moreover, the interception shall be carried out to achieve the authorized purpose only.
- In the interests of state security or to prevent, investigate, or prosecute a cognizable offence, the Chief Privacy Commissioner may order the communication to be intercepted. Before granting the order, the Chief Privacy

> Commissioner must ensure that "all other permissible options of obtaining the information sought to be intercepted have been exhausted" and that the planned interception is "reasonable, proportionate, and not excessive."

Some people believe that there is no clear definition of the term "informed consent" in the proposed Bill. Unless people are aware of the consequences of a data breach, they are unlikely to give informed consent. The bill did not consists of any regulations on CCTV cameras or codes of conduct for users of mobile cameras. The 2013 law left did not took into account many crucial issues and many field remained unanswered. The most important unsolved issues include uncontrolled use of technical skills and observation of disruptive technologies. The argument over the level of surveillance that users should be subjected to did not take place inside or outside the parliament. Bill remained silent on political organisations, as well as prospective 'targets' doing sensitive tasks such as judges, opposition leaders, editors, regulators, activists, vigilance authorities, corporations, and others.[66]

Researchers of this work claims that in the 2013 bill, terms such as "public order" and "preventive incitement to the commission of an offense" are not very clear in their approach and vague in nature but however these terms has broad ambit. In addition, the entire mechanism of intercepting communication requires judicial review.

[66] Shalini Singh, "Lethal surveillance versus privacy," available at http./Avww.thehindu.com/opinion/lead/lethal-siuveillance-versus-privacy/article4837932.ece

CHAPTER-4

INFORMATIONAL PRIVACY IN THE TECHNOLOGICAL WORLD

4.1 Introduction

Since the entire universe contains a vast ocean of information, only enlightened people can understand it. Even on our Earth each and every substance gives detailed information about its composition, shape, structure, advantages or disadvantages etc. As per the famous theory of Human nature which is extended by Aristotle, individuals in the universe are composed of matter and form. Therefore, matter and information are an important part of every physical thing in the Universe. [67]

Aristotle's description of perception shows that all animals are information processing organisms, and their body structure explains the way information is processed in them. Aristotle explained that the processing of information in animals initiates and controls their behavior. Humans can also be ranked as a information possessing organism but humans are blessed with the capability to think about their actions and have rational approach and this makes them ethically responsible for what they do and what they become.[68] It is submitted that human Beings have been transforming the information since past times. It would have been impossible for any civilized society to survive, if it could not gain the past records or information.

In order to facilitate the social management information systems, urban information systems, health information infrastructure, business document systems, and survey databases that mainly contain personal and social data have been structured and developed. Personal data has become an essential raw element in today's social economic activity. Critical business goods, services, operations, and responsibilities for

[67] Terrell Ward Bynum, "The Historical Roots of Information and Computer Ethics" , in Luciano Floridi (ed.), The Cambridge Handbook of Information and Computer Ethics, 20-38 at 23
[68] *Ibid.*

a vast number of public and private organisations necessitate the accurate use of personal data.[69]

Without a question, the collecting and utilisation of personal information has become a major role in the evolution of society as a whole. However, several privacy issues have been jeopardised as a outcome of these advancements.

4.2 Meaning of Informational Privacy

"L. Floridi" defines informational privacy in these terms: *"freedom from epistemic interference or intrusion, that is achieved when there is a restriction on facts about someone that are unknown or unknowable".* Judith Wagner Decew further added to the concept and said that*"The 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 need not divulge and can expect others to guard as well".*[70]

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".*[71]

4.3 Role of Technology in the Process of Data Collection

In was in year 1973, the team introduced computers and data protection to "US Secretary of Health, Education and welfare (HEW)". This report can be written today: no wonder people did not seemed to believe in computerized bookkeeping. In private settings, as the relationship between providers and recipients of personal data becomes weakened, impersonalized and blurred as individuals have weaker control over the personal data they transmit to any organization and that is extracted by the organization. A person's information is usually obtained through personal contact, which requires

[69] James B. Rule, "Toward Strong Privacy: Values, Markets, Mechanisms, and Institutions" , 54 University ofToronto Law Journal, 183-225, at 183
[70] Judith Wagner Decew, In Pursuit of Privacy: Law, Ethics and the Rise of Technology, 75 (1997).
[71] Herman T. Tavani, 'informational Privacy: Concepts, Theories, and Controversies," in Kenneth Einar Himma and Herman T. Tavani (eds.), The Handbook of Information and Computer Ethics, 131-164 at 140

personal trust and a certain symmetry or balance between the provider and the recipient. Sometimes a person does not even know that the organization is keeping their records. Many times, you may not see it, let alone doubt its accuracy, observe its spread, or suspect that other people are using it.

The report points out that the problem is not only caused by the powerful computer technology that can be used for good and evil, but also by their impersonal qualities. The problems of this era are not outdated. We are still dealing with databases that contain too much information to be easily accessible; databases that contain inaccurate information; and the use of data in databases created for legitimate purposes is not so noble, if not completely unethical.[72]

The computer-assisted revolution in man's ability to process data is clearly a huge benefit. Men can now make more fact-based, logical, and predictable judgments in business, government, medicine, research, and a dozen other professions than they could before the advent of electronic information storage and retrieval.[73]

Electronic digital computers have supplanted traditional means of information collecting. More records can now be stored and manipulated more effectively and quickly than ever before thanks to recent technological advancements. Every organisation collects information about its employees, clients, members, taxpayers, and other persons in the business's interest utilising massive computers.[74]

New up gradation in computer technology are quickly accelerating data exchange between machine users. The standard growth of computer languages and the improvement of the machines that translates machine systems from one machine to another have allowed computers to connect and communicate directly with each other so that data can enter and exit separate systems. This innovation has led to the exchange of information between departments of the same large organizations as the police force and state health authorities or between independent organizations having common goal and objective such as life insurance companies. A more significant aspect of this

[72] Jonathan Zittrain, The Future of the Internet And How to Stop It. 201
[73] Alan F. Westin, Privacy and Freedom. I 58 (1970).
[74] *Id.,* at 161.

trend is the growth of central data pools in many important fields, from education and health to banking, civil defence, and social-science analysis.[75]

Meanwhile, it is pertinent to mention about Data-mining, which is being considered as the revolution in the information technology.

Due to the widespread availability of huge volumes of data and the unavoidable need to transform these data into valuable information and knowledge, data mining has recently gained a lot of interest in the information industry and even in society. Market analysis, fraud detection, and consumer loyalty, as well as production control and research and development, can all benefit from the insights collected. In simple terms, data mining is the process of extracting useful facts and conclusions from a large pool of data held in databases and other data storage sources

Simply described, data mining is the application of statistical tools to vast amounts of data in order to uncover previously unknown associations. Data mining can be used for ranking purposes, such as assessing whether a person belongs to a specific group or making predictions.[76] For example, this means strategic research and analysis of personal life files in order to derive information about a person's tastes, preferences, behaviours and attitudes and at last conclusion is drawn out. There is huge commercial use of data mining like by educational institutions, health infrastructure, advertising companies etc.

In light of the aforementioned issues, the European Union has identified three major developments that will constitute a future risk to personal data protection. The first danger stems from modern technology's incredible powers. Second, the rising internationalisation of data flows raises privacy concerns. Third, law enforcement officials now have greater access to personal data than ever before, putting an individual's liberty at risk.[77]

Technology itself self don't infringe on anyone's privacy. It is the people who use the technology and the policies use technology as a tool to infringe upon others privacy. Many people advocate giving up a certain degree of secrecy in order to enjoy the

[75] *Id.,* at 162.
[76] Patricia Oslund and Larry Hoyle, "Data mining" , in William G. Staples (ed.). Encyclopedia of Privacy, 159-161 at 159
[77] Viviane Reding, "Tomorrow's Privacy" , International Data Privacy Law, (2011), vol. 1, No. 1, 3-5, at 3.

benefits of modern society. From their perspective, it must be recognized that credit card transactions inevitably record data on our buying and driving habits in a large database beyond our control.

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.

4.4 Collection of Personal Records by Private Entities

Daniel J. Solove wrote:

"Businesses are collecting an unprecedented amount of personal data, recording the items we buy at the supermarket, the books we buy online, our web surfing activity, our financial transactions, the movies we watch, the videos we rent, much more. Nearly every organization and company we interact with now has tons of personal data about us. Companies we've never heard of also possess profiles of us".

Firms and other organizations generate a lot of data. Almost every private sector is using technologies and softwares, and the firms have turned to mining their own proprietary databases. It is because of the fact that the price of such technologies is being continuously decreased. If a database has information for many variables on many people, it is possible to look for useful correlations. Most public attention has been focused on the retention of data about customers, but companies also collect data about their own products, their employees, or the companies they do business with.

The interesting aspect is that the information itself has become a valued property. A mailing list is nothing more than a mailing list. The value is in the information it contains like potential customers' names and their addresses. There is nothing new about selling mailing lists or about keeping careful records. But today computers are able to combine large datasets into a single database that can be mined to extract commercially useful information. Therefore, the commodification of information and the ability of computers to manipulate informational data has become potential threat to individual privacy.

Earlier, only the government was interested in collecting the personal data of social and economic importance. But since the early 1990s, private sector has vastly been engaged

in such transactional data systems. Sophisticated strategists in the industries like consumer credit, direct marketing, insurance, and publishing, enhanced profit by tailoring the consumers' personal data.

In the cyber age, everybody inevitably leaves trails of his personal information and hence, such personal data provides the infinite opportunities to organizations to make calculated appeals to specific individual for commercial transactions. Therefore, commercially motivated organizations exhaust every resource for Target Marketing and Target-Pricing. In Target-Pricing, sellers adjust their prices by watching the consumers' previous purchase history.

Consumers are obvious participants in the behavioural target marketing process. Consumers are careful about their personal information. Their lack of autonomy is harmed by their unintentional sharing of knowledge. Such obtrusive selling affects their family's tranquilly. Surprisingly, customers are unaware of the information they provided to marketers..[78]

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.[79]

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 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.

Some information is uploaded to websites or blogs voluntarily by individuals, so it is publicly available. Other information can also be provided voluntarily, but it is not known that this information may have a wider range of uses than the provider expects.

[78] Ellen R. Foxman and Paula Kilcoyne , "Information Technology. Marketing Practice, and Consumer Privacy: Ethical Issues" , Journal of Public Policy & Marketing, Vol. 12 (I), (Spring 1993), 106-1 19, at 108.
[79] Malcom Warner and Michael Stone, The Data Bank Society, 68 (1970).

Certainly such practice aggravates the problem when the data is inaccurate. Data may be incorrectly entered into a database. An innocent person can be falsely arrested if law enforcement database recorded wrong information about him.

4.5 Consumers' Privacy

4.5.1 Online Consumers' Privacy

A lot of users don't realize that they are exposed to privacy threats from cookies when interacting with websites. Cookie technology authorises the website owners to gather data about users' browser preferences when users use their website.

Cookies refers to that piece of data or information which is transmitted from the server of the web to the users browser. These information could be in form of login details, data about users preferences and choices etc.

In the Behavioral marketing or targeting, the companies collect and compile the internet users' online records. As a result, businesses keep track of people's web browsing history, interactions on social networking sites, email content, and purchases of goods and services. They can then deduce the consumers' tastes, preferences, behaviour, or interests and sell their products appropriately.

4.5.2 Access to Mobile Phones' Personal Information

In the history of the collection of personal information, the first revolution took place in the form of computer technology which actually replaced traditional modes of collection. Usage of Mobile phones during past decade also strengthens the bridge between communication and information. Obviously, people do have strong expectation of privacy while communicating and transacting information with each other.

Such mobile phones, on the other hand, have progressed from simple headsets to Smartphones with complex applications. These programmes can interact with and retrieve information from many functionalities on the phone, such as the camera and address book, once they have been installed by the user.

Such "applications" , in short term, are known as "apps". The "apps" are in the form of games, utility or any other type of program including basic torch on phones, weight-loss guide, wallpapers and Global Positioning System (GPS) softwares. Usually the app

developers tag some unclear "terms and conditions" with the applications and seek users' consent. No doubt users get fascinated with new softwares and applications, and hence, install the applications by agreeing their unclear terms and conditions. By agreeing, the users grant license to apps agreed that App developers and their advertisers now have access to their phone. With this they can now read users' text messages, harvest e-mail addresses, take images from the camera at any time, dial any number from users' phone and intercept the calls, and access users' web browsing history. Unfortunately, every multi-national internet giant like Facebook are engaged in such malpractice. The apps of Facebook, twitter, or others are being downloaded to Google Android phones, Apple's iPhone, etc. and hence, accessing the private information of users.

In order to protect users' personal data from malicious smartphone applications, smartphones need a new privacy setup. Privacy mode can be effective enough to prevent (or configure) applications from accessing personal data stored on the phone. If users want to install an untrusted third-party application, they can optimize access to the application to indicate what types of private information (such as device ID, contract, call history, and location) can be used by the application. In addition, users can flexibly (re)configure previously granted access rights at runtime (for example, during installation).

4.6 Users' Personal Information on Social Networking platform and Privacy Issues

For every democratic nation, it is necessary that informed citizens should participate in the making of any public policy. Obviously, the social networking sites have provided much better platform for such participation than real world ever possessed with.

According to Barnes, *"Social networking sites are a group of Web sites that provide people with the opportunity to create an online profile and to share that profile with others".*[80]

[80] Dianne M. Timm and Carolyn J. Duven, "Privacy and social networking sites" , in Special Issue: Using Emerging Technologies to Enhance Student Engagement, Volume 2008, Issue 124, (Winter 2008), 89-101, at 89. Available at http://onlinelibrary.wiley.com

Indeed, educational institutions are recognising the value of social networking platforms in engaging students in creative and thought-provoking ideas. Academic libraries, enterprises, including hospitals, and other organisations are similarly interested in networking tools and apps since sharing knowledge and finding specialists is vital to the organization's success. Musicians, in particular, are promoting themselves on social media networks.[81]

The social networking sites require every user to sign up first. At the time of registration, the users at least submit their names or usernames. Later, in the site, the users make a profile which consists of detailed personal information and preferences. All users voluntarily upload their pictures, family pictures, videos, etc. on the sites like YouTube and facebook. Similarly, the users express their feelings, ideas, comments, etc. by way of blogging at the sites like Twitter.

Despite its social benefits, the usage of social networking sites has also raised many privacy issues. People are using these sites without any sense of responsibility and hence, infringing each other's privacy rights. No doubt, blogging and uploading pictures or videos come within the ambit of freedom of speech and expression. People are aware about such restrictions in the real world, but have forgotten them in the virtual world. If there is no public interest involved, a person cannot publish someone's picture or video without latter's consent.

Furthermore, because of the widespread accessibility of the virtual world, privacy intrusions on social networking sites have damaged individuals in both physical and psychological ways. By recounting the storey of "Dog poop girl," Daniel J. Solove demonstrated the psychological impact. When a girl refused to clean up her dog's faeces on the train, she was given this nickname. The fellow passenger captured her image along with dog's excrement on the floor of train. The image, then, was disseminated in the internet world. Due to the widespread of image, the girl felt humiliation and embarrassment. It seems that she was punished disproportionately and unreasonably in the virtual world.

Unfortunately, majority of users don't even aware about their own privacy issues in the virtual world. Users' privacy and reputation may be jeopardised by information shared

[81] Melissa L. Rethlefsen MLS, "Social Networking." Medical Reference Services Quarterly, 26:S1, 117-141 at 120

on social media. Surprisingly, such personal information is being used by companies, employers, anonymous cyber-stalkers, and the governments. It has been revealed that the social networking sites are selling the personal data of its users to third parties, in consideration of huge amount of money. The companies, who bought personal details, can easily decipher the taste and preferences of the users. Hence, they use it for behavior target marketing. Increasingly, news headlines reveal that people have lost employment, college admissions, or relationships as a result of uploading images shot while inebriated.[82]

Furthermore, material uploaded on social networking sites is accessible to both users and non-users, and is even searchable by search engines like Google. However, this does not imply that users are unconcerned about their privacy. The problem is the lack of knowledge regarding the new softwares, applications, and technologies. The users often hurriedly adopt new social media tools without considering service providers' capacity and potentiality to collect the personal data of its users. Therefore, it has become necessary on the part of the social networking sites to inform the users about the consequences of the choices, and clarify the trade off between publicity and privacy. Such kind of awareness may enable the users to make free and informed choices.

With the increase in the use of social networking sites, the users are being victimized by the anonymous cyber-stalkers. When the users upload their personal details on the internet, the cyber-stalkers watch users' every update and determine the taste, choices, behavior of preferences of the users. It was reported that, by using details, the cyber-stalkers set up the sex profile in user's name. This led to harassment for the victims. Police and criminal justice system is still weak in dealing with such matters. However, Facebook and other social networking sites are working with police and trying to capture the malicious people. Facebook claimed that whenever an abuse is reported, they react swiftly to review the malicious content and disable the fake accounts.

4.7 Medical Privacy

Since the introduction of the Hippocratic Oath around 400 BC, Protecting patient privacy has become an crucial part of the doctor's code of conduct. Over time, medical information is used by many organizations and individuals that do not comply with

[82] OmerTene, "Privacy: The new generations," International Data Privacy Law. (2011) 1 (1): 15-27, at 23, available at http://idpl.oxfordjournals.Org/contcnt/l/l/15.full.pdf-html

medical ethics Codes and those includes employers, insurance companies, government plan administrators, lawyers, etc. As the use of health information increases, so does the government's protection of this highly confidential and very personal information.[83]

Since the relationship between doctor and patient is fiduciary one, it becomes necessary on doctor's part to keep the confidentiality and privacy of its patient's health records. Over the period of time, the healthcare has become the huge source of one's sensitive information. Health care providers, companies providing medical services, medical health organizations, etc., collect and collate the huge amount of patients' health information. Obviously, disclosure of one's personal health report could cause an embarrassment to him. Moreover, such personal health information can be exploited discriminatorily by life insurance companies, employers, or by any person in many avenues of life.

However, the Punjab and Haryana High Court in the case of Surjit Singh Thind v. Kawaljit Kaur,[84] court underlined and well established that examination of a woman virginity upon marriage is a clear violation of rights granted under Article 21 of the Indian Constitution.

4.8 Right to Information vis-a-vis RTP

As per the Indian Laws , citizens right to gather data about public matter is a part of article 19 of the Indian Constitution.[85] In this sense, it is clear that right to get information from public authorities is very important for every democratic set up. However, it raises the question that whether an individual has full access to all public documents? Obviously, privacy advocates want justified answer.

The right to information is a privilege, not a right. The Parliament has the authority to impose reasonable restrictions on the "right to information" in the interests of India's sovereignty, integrity, and security, international relations, public order, decency, or morality, or in connection with contempt of court, defamation, or incitement to a crime.

[83] "Medical Record Privacy" available at http://epic.org/privacy/medical
[84] AIR 2003 P & H 353
[85] Dewan, Exhaustive Commentary on the Right to Information Act, 2005, 32

It indicates that in order to defend one's right to privacy, one's access to information can be reduced.

RTP is not specifically mentioned in the Indian Constitution, but it was unanimously recognised as a Fundamental Right under Article 21 of the Constitution in the well-known case of Justice Puttaswamy v. Union of India.

In one of the most well-known cases, People's Union for Civil Liberties v. Union of India, the Supreme Court of India clearly stated that the Indian government's tapping of phone calls in the exercise of Section 5 of the Telegraph Act is a clear violation of the right to privacy guaranteed by Article 21 of the Indian Constitution.

4.8.1 Publication of Judicial Proceedings

According to a journalist, what is public knowledge to others could be personal and sensitive information to a party in a marriage conflict lawsuit. So far as court records are concerned, they are not accessible every time. It means that every court record is not accessible, and subject to certain exceptions. Many times, a statute or an enactment itself prohibits the publication of the proceedings which is being regulated under that statute or enactment. Moreover, it is upon the court to decide whether any of its judgment is reportable or not. In the matter of R. Sukanya v. R. Sridhar, the Madras High Court decided that S. 22 of the "HMA, 1955" acknowledges the right to privacy between the parties in a Hindu Marriage Act procedure. The court emphasised the section 22 requirement, which clearly states that all proceedings under the Act must be conducted in secret. The provision continues to state that it is illegal for anyone to print any matter connected to such records, and that anyone who violates this prohibition faces a fine of up to one thousand rupees. Undoubtedly, the matrimonial matters which are very sensitive and personal matters, have no relation with the public interest and public affairs. Therefore, the press is lawfully prohibited to publish or telecast such personal matters.

Furthermore, another question arises as to whether the identity of the victim of rape or sexual offences should be disclosed in the public. The answer must be in negative. The Supreme Court of India considers sexual violence as degrading act and a violation of female's right to privacy. A rape victim goes through misery and a horrific crisis. The publication of the victim's or her family member's name, identify, or photograph in such a case may expose her to secondary victimisation. Furthermore, the IPC, 1860, makes

it illegal to reveal the identity of a victim of certain crimes. In the case of High Court or Supreme Court judgements, however, the prohibition on publication does not apply. However, in recognition of the victim's social victimisation in cases of rape or other sexual violence, the Supreme Court ruled that all lower courts, High Courts, and the Supreme Court itself should not use the victim's name in their decisions.

Despite the persistent and prevailing friction between 'right to know' and 'right to privacy' , the Supreme Court's judgment of R. Rajagopal v. State of T.N is somehow a guide for every advocate. In this case, the Supreme Court showed its great concern to balance between these two countervailing rights.

4.8.2 Cyber Crimes Invade Informational Privacy

Computer crime can be generally defined as any criminal conduct committed with or without the use of a computer. This encompasses unlawful access to or use of information systems, as well as programme modification for profit or malevolent intent..[86]

Hacking is the most visible kind of computer crime, which comprises using the telephone system to gain unauthorised access to computer systems and their data. The search for access codes is known as hacking. To evade detection, this search can be random or employ extremely complex procedures. Manual hacking, using only a telephone is also known as finger hacking and is the technique of trying number after number until a valid access code is detected. Computer hacking uses computers programmed to dial target numbers and to search for access codes either sequentially, randomly or algorithmically.[87]

Criminals have created a variety of methods for gaining illicit entry into computers, sometimes from the same site and usually from a faraway place. Viruses, worms, and Trojan horses are among the most common ways for remote entry into systems..[88]

Viruses are computer programmes that alter other programmes and replicate indefinitely, infecting additional programmes. The virus enters the computer system through an infected software, which then replicates by instructing the host programme

[86] William J. Martin, The Global Information Society, 106 (1995).
[87] *Ibid.*
[88] *Id.,* at 107.

to inject code fragments into other programmes, much like biological viruses do. The infected programmes continue to transmit the virus until the infection has progressed far enough that the viruses become active and destroy all software on the system..[89]

A worm is a computer software that replicates and spreads from one machine to the next. A worm is a programme that runs on its own. It is well adapted to 'sneaking' from one computer location to another. Once the work has infiltrated the target computer system, it has the potential to leak information to the outside world, harm the system, or simply become a nuisance by slowing the machine down. A worm is the most technically advanced type of computer attack. It's the least likely to be discovered and excels at leaking critical data.

No doubt, Internet has improved the mode of communication and advanced the level of education, but it is still largely unregulated. Laws relating to online privacy are under development. In the virtual world, various malpractices are violating an individual's informational privacy. Another major problem in the cyberspace is the problem of identity theft and phishing. In identity theft identity of the user tried to be copied by data theft to do malicious act .

Cybercrime like identity theft has countless repercussions. It is not only confined to financial harm but victim's everyday life will be affected. The dossiers of personal information, once polluted by thief, will continue to harm the victim if police fails to arrest the culprit. Further, such crime is a social problem. The terrorists' engagement in identity theft is serious threat to the security of people. The identity theft also results into the losses to creditors, financial institutions and companies.[90]

4.9 Privacy Enhancing Techniques

Privacy-Enhancing techniques have been devised for internet users so that they can have control over their personal data. It also enables users to record, archive, and search for their past personal data transfers, including when, to whom, and under what conditions. It also knows the rights of users to view, correct, and delete data.

Herbert Burkert defined "Privacy Enhancing Technologies" ("PETs") as:

---

[89] *Ibid.*

[90] Daniel J. Solove, "Identity Theft, Privacy, and the Architecture of Vulnerability" , 54 Hastings L.J., (2002-2003), 1227-1275. at 1245.

"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".[91]

A. Michael Froomkin argued that although use of privacy-destroying machineries by administrations and trades has threatened an individual's informational privacy, everything is not lost yet. Advancement in science and technology has decreased the costs of data collection and increased the quantity and quality of data. He said that privacy -destroying technologies can be responded by deploying privacy-enhancing methods and other privacy shield know-hows in a scheme plan. In addition to privacy-enhancing techniques, some other techniques can also be used by people for self-help. Such technologies may either hardware or software. Among hardware there are devices like masks or thick curtains. Similarly some softwares like Platform for Privacy Preferences ("P3P").[92]

Many ways have been developed to increase data security in order to secure data. Users can only access data at their allowed level if the database uses a hierarchical security model to classify and restrict data according to different security levels. Another approach that can use a single data element is encryption. Encryption protects personal information from being leaked.

Privacy data mining is a new topic of data mining research that arose in response to concerns about privacy in mining. It's also known as privacy-sensitive data mining. Its goal is to get trustworthy data mining findings without knowing the value of the underlying data. Secure multi-party computation and data obscuration are two general ways.

It is submitted that both public and private agencies have widened their processes of collecting individuals' personal information for multiple purposes. However, the information processors have failed to provide adequate security to the collected personal data. Similarly, law is either inefficient or insufficient to adjust the gathering,

[91] Herbert Burkert, "Privacy Enhancing Technologies and Trust in the Information Society (1997)," Quoted in A. Michael Froomkin, "The Death of Privacy?," Stanford Law Review, Vol. 52, No. 5, 1461-1543 at 1529.

[92] A. Michael Froomkin, "The Death of Privacy?," Stanford Law Review, Vol. 52, No. 5, 1461-1543 at 1529 (May, 2000

collation, storing, or disclosure of private data. Therefore, answer to the problem lies in both technological and legal solutions.

Chapter 5

FREEDOM OF MEDIA AND RIGHT TO PRIVACY

5.1 Introduction

Freedom of speech is considered to be one of the most important concepts for the development of individuals and the entire society. If people cannot express their political beliefs and opinions freely through open discussion and response to other people's criticisms, they will not be able to develop intellectually and spiritually.[93] Disclosing the truth for the public good and people's participation into the democracy via freedom of speech make the government's actions more transparent and accountable. At present, with the installation of new technologies, like internet, mobile technologies, etc. the scope of traditional "press" , which included only print media, has become enlarged in the form of electronic media. Consequently, the responsibility of the "media" has also been increased. Therefore, the term "media" includes both print media and electronic media. The print media is largely depended upon for news and views and only marginally for entertainment, whereas the electronic media has been looked upon as the chief source of entertainment though increasingly it is also being resorted to for news and views. Together the print and the electronic media today embrace almost the entire section of the society. They have succeeded in crossing the barriers of poverty, illiteracy and even geographical inaccessibility, due to community libraries and reading rooms and the community Television and radio stations. Together they have a wider reach and a more effective and a more direct approach to the people. In fact, there is no institution in the society which has the approach to and the intimacy with the people as these two institutions. That is why the media has come to be looked upon as the fourth pillar of the society along with the other three pillars.[94]

Simultaneously, with the increase in the accessibility, media's responsibility towards the society has also been increased. Freedom of media has therefore to be used in a manner which will respect the rights of individuals and will not interfere with the functioning of the other institutions by undermining the confidence of the people in

[93] Eric Barendt, Freedom of Speech, 14 (1987).
[94] P.B. Sawant, Mass Media in Contemporary Society, 68 (1998).

them. The freedom has also to be used to guard and promote the benefits of the humanity. Self-restraint, self-discipline, a sense of duty and responsibility to the society must therefore mark the exercise of the freedom.[95]

It is well knowledge, however, that freedom of speech and expression does not fall under the umbrella of absolute rights. In general, the right to privacy and the freedom of speech and expression are closely connected.

5.2 Investigative Journalism and Privacy Issues

So far as the tussle between media and privacy is concerned the story started with the publication of an article entitled as "Right to Privacy" in the year 1890 by the two Boston lawyers named as "Samuel Warren and Louis D. Brandeis". The authors criticized the malfunctions of the press. They observed that the press is exceeding in each path the obvious bound of decorum and of politeness. With the commercialization of the press, the Gossip and details of sexual relations became the breaking news. It was argued that due to the complexity of life, a man has become more sensitive to publicity and hence, he needs solitude and privacy.

Therefore, with the increase in the science and technology, the journalists have well equipped with privacy invading techniques like miniature cameras, bug devices, etc. And these are very potent tools for investigative journalist who conducts the sting operations. Simultaneously, such potential also increases the responsibility of the journalist to do stings in public good only.

In past, the press played the significant role during three moments-the Civil Rights Movement, the Vietnam War, and Watergate. During this period, the courts also favoured freedom of press because the journalists had public regard.[96] This was the time when investigative reporting was really doing something for public good. Whereas, today's media is more concerned about their Television Rating Point (TRP) ratings and showing news regarding celebrities only, which doesn't reflect any 'public good'. The reality television (TV) shows spreading the indecent values in the society. Hence, the media is losing the public support.

---

[95] *Id.,* at 94.

[96] Amy Gajda, "Judging Journalism: The Turn Toward Privacy and Judicial Recognition of the Press," California Law Review, Vol. 97: 1039: 1039-1105 at 1068,

The landmark decision of Supreme Court in the well-known situation of New York Times V. Sullivan provided a more important impetus to journalists' demands for constitutional privileges. Because the plaintiff, as a government employee, must prove that all lies in news stories are based on malice or reckless disregard for the truth, this ruling has created roadblocks in the resolution of defamation complaints against journalists. The press guarantees that politics, institutions, and an open society are preserved.

Investigative journalism refers to a type of news in which reporters carefully study an interesting topic, usually related to crime, political corruption, or other scandals.

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.

In the history of investigative journalism, the famous instance is of "Watergate".However, with the passage of time, Reporters forgot their moral responsibility in finding the truth. Investigative reporters often use various means for their fact-finding like surveillance techniques, miniature cameras, phone records, phone tapping, etc. Many times they even adopt the illegal means to investigate the matter. Obviously, such kind of uses makes the action punishable under the Indian Penal Code. For instance, in Tehlaka' s Operation Westend case, the undercover journalists used the prostitutes to expose corruption in defence deals.[97]

String operation strengthens the democratic fabric of a nation by disseminating information about important public interest events that cannot be easily obtained through simple inquiry or effort, thereby serving the public interest. However few of the recent incidents provides for the proof that string operation is misused by by the media and private organizations to expand viewers on their network, resolve political bills, harm corporate interests. This type of string operation has the capability to

[97] Ramachandra R. Kothapalli, "Operation West End: A Case Study in Media Ethics," Media Ethics, available at http://www.mediaethicsmagazine.com/index.php/browse-back-issues/l35-fall-2008/36438l3-operation-west-end-a case-study-in-media-ethics

undermine commons belief in establishments and generate a cynical environment in society.[98]

In India, the judiciary has played a key role in establishing press freedom as a basic right. Although the Indian Constitution lacks an express provision for "press freedom," the courts have succeeded in making it an implicit provision by liberally construing Article 19(1)(a) in conjunction with Article 21.

However, the Indian courts did not formulate a clear policy or uniform method on legality and admissibility in the "Operation Sting" case. However, some general principles can be emphasized, such as public interest considerations and protection the fundamental rights of the 'Targets' of string operation. In addition, Indian courts have recognized the inherent illegality of publishing/displaying fabricated and misleading content received from Sting Operation, which has been condemned in almost each and every country of the world .[99]

In the absence of any strict regulation, the principles of self regulation in journalism are of worth mentioned over here. Regarding the concept of String Operation:

"As a guiding principle, 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 substances or any act of violence, intimidation, or discrimination as a justifiable means in the recording of any sting operation. News channels will as a ground rule, ensure that sting operations are carried out only as a tool for getting conclusive evidence of wrong doing or criminality, and that there is no deliberate alteration of visuals, or editing, or interposing done with the raw footage in a way that it also alters or misrepresents the truth or presents only a portion of the truth".

Furthermore, the Indian Law Commission has noted that the media, using modern technologies, is conducting sting operations to expose corruption, immorality, exploitation, and violations of the rule of law by individuals in positions of power, powerful people, and companies. However, at the same point of time, the media is also

[98] www.lawcommissionofmdia.nic.in/stingoperation.doc
[99] *Ibid.*

accused of doing stings for commercial purposes. This led the journalists to make the news more sensational and emotional.

On August 28, 2007, Live India (Janmat) (TV news station) aired a sting operation covering a porn racket run by a schoolteacher in Delhi involving schoolgirls as part of one of the negative sting operations. In the footage, a school teacher named Uma Khurana is seen haggling with a customer (undercover journalist) who wants a girl's "services." He gave her Rs. 400 and she turned over a 15-year-old girl who was an ex-student at her previous school.[100] She faced mental agony, suspension and termination from the services. But later on, after police investigation it was discovered that the whole sting was wrong. The police found no concrete evidence regarding Uma Khurana's involvement in child prostitution. Therefore, she was reinstated in her job. But due to this sting operation she lost her reputation and self-respect. During mob violence her modesty was also outraged.[101]

As a result, press freedom is not an absolute right in our culture. Every judicial system has the authority to impose reasonable limits on reasons such as contempt of court, incitement to commit an offence, state security, public decency and morality, defamation, and the protection of privacy rights, among others. Phone tapping, in a similar vein, has been viewed as a major violation of one's right to privacy. In India, only the government has the right to intercept any communication under Indian Telegraph Act of 1885. In PUCL v. Union of India1, the Supreme Court of India has issued certain guidelines to regulate the practice of phone-tapping like, permission from home ministry is required for every interception, the issuing authority should maintain the complete record of intercepted material, etc. Hence only government can intercept the telecommunications and private individual does not have any right to tap our phones.

The court found that if the media has unlimited and unregulated freedom to post photos of suspects or defendants before performing identity verification, or if the media releases a statement that suspect is guilty , there is a serious risk of injury if such things are done before the court issued such an order.

[100] http://en.wikipedia.org/wiki/Live_India
[101] Court on Its Own Motion v. State, 146 (2008) DLT 429. Available at http://indiankanoon.org/doc/45618/.

It is submitted that Investigative journalism must be used in a legal manner. First the journalists should exhaust the lawful methods to access the things. For example, under right to information one can access any public record (obvious exceptions are there). The journalists can analyze all records and can make their case. After doing this the journalists should prove before some authority that there is a reasonable case and it is in the interest of larger public to conduct sting operation. No doubt, journalists are using very sophisticated bug devices which have the potential to intrude into anyone's private life. But they should not forget the journalism ethics in conducting any sting operation. Therefore, it has become very necessary to codify the uniform laws for regulating the sting operations.

As the researcher observed, investigative reporting essentially intends to be conducted for public good. In fact, the pristine concept of investigative journalism was emerged to bring public accountability and transparency. At the time of the birth of investigative journalism, journalists' work used to be admired by the courts as well as general public. Indeed, sophisticated bug devices also enhanced the journalists' potency to conduct sting operations. However, today's media is more concerned about their Television Rating Point (TRP) ratings and, conducting sting operations for commercial purposes only. This also led the journalists to make the news more sensational and emotional. Recently, television networks have gone beyond the pale of morality by employing sting operations as a technique for ongoing reality shows to uncover adultery of a spouse, lover, or other loved one. The importance and relevance of sting operations has been diminished as a result of such TV reality shows. Another issue is the constant broadcasting of sting operations, which produces a large public perception of the accused's guilt and may influence the decision of the trial court judge who is hearing the case. Furthermore, the media's over-inquisitiveness about celebrities' personal lives has contradicted the goal of media independence. The news regarding celebrities' private lives serve no public good. It is because of this reason that the media is losing the public support. Therefore, it is submitted that the pious and sacred concept of "investigative journalism" should be used to promote the democratic values of the society. The journalists' should respect the decent values of civilized community. They should not spread the sensationalism for the sake of commercial purposes. They should not forget the professional code of ethics in conducting sting operations. The recordings

of sting operations should not be altered or edited. The editor should decide judiciously in broadcasting any kind of sting operation and, consider its implications also.

5.3 Media Laws in India

It is submitted that freedom of media is not absolute and, the Parliament can regulate it by imposing reasonable restrictions on it. Freedom of media includes print media as well as electronic media.

5.3.1 Legal Framework for Press

The Indian press is vigorous, activists, and pluralistic constraints, which include laws governing the operations of the press, demands of advertising, labour conditions, government control and regulations of newsprint, activist role of the owners, and institutionalized regulations through such bodies as the Press Council and the Press Commissions.

Article 19(1) of the Indian Constitution guarantees freedom of speech and expression (a). Under Article 19(1), the Supreme Court of India has ruled that freedom of speech and expression encompasses freedom of the press (a). Article 19's sections (2) and (6), however, place some restrictions on this privilege. Clause (2) allows for restrictions on public order, good international relations, and criminal encouragement. Clause restricts the right to practise a profession, employment, trade, or business (6). The Supreme Court, on the other hand, has the authority to review the law and to strike down unjustified limits.

The major laws that potentially affect the operations of the press include:

- Criminal laws, particularly those in S. 144 of the IPC, intended to maintain public order. Penal Code provisions on Sedition (Section 124 A), promotion of class hatred (Section 153 A), obscenity (Section 292), Defamation (Section 499), and “public mischief” (Section 505) also apply to the press.
- The court has power under the “Contempt of Courts Act, 1971” to restrict the publication which lowers the authority of the court and interferes with judicial proceedings or obstructs the delivery of justice.
- Provisions pertaining to the press and the legislature, including rules that empower speaker to regulate the entry of non-legislators to legislative proceedings and privileges relating to the publication of these proceedings.

- The Indian Officials Secrets Act, 1923 prohibits the gathering and publication of any sketch, plan, or note that an enemy state could use.
- General laws on taxation in so far as they do not "single out" the press and place any unfair burdens to limit circulation of the press.
- The Indian Post Office Act 1898 regulates the transmission of "indecent or obscene" material and seditious matter, and allows for interception in the interest of public safety.
- Laws that regulate industrial relations, as well as those relating to operations of business, also apply to press.
- The "Payment of Wages Act 1936" and the Working of Journalists (Conditions of Service) and Miscellaneous Provisions Act- both of which deal specifically with the working conditions of journalists.
- The Copyright Act 1957 protects intellectual property under certain conditions.

Besides the legislations, the government also institutionalized regulation of the press through several bodies i.e. the Press Commissions, Press Council, and the Office of the Registrar.

5.3.2 Legal Framework for Broadcasting

Television commenced in 1959 as an educational experiment involving television clubs in New Delhi where some 21 community TV sets received the programs. Regular broadcasting was introduced in New Delhi in 1965. The expansion of the medium was tentative with about a dozen cities receiving TV signals by 1975. From such a modest beginning, starting in 1982, the TV system has expanded into one of the main systems in the world. Indian television is modeled on the European model representing a strong network dedicated to public service and a number of private satellite channels primarily offering entertainment programs. This "mixed" model offers a challenge to regulators.

Article 246 of the Indian Constitution, as well as other laws such as the Indian Telegraph Act of 1885 and the Indian Wireless Service Act of 1933, give the government power over broadcasting. The parliament is empowered to enact various legislations relating to the subject of broadcasting and communication. Article 19(2) which is a part of golden triangle of the constitution of India governs the present

Broadcasting policy of the country. However provisions bounds the Broadcasting companies with many tems and conditions such as they would not criticize those countries who are friendly with India or speak on religious sentiments of a community ,incite violence, and the like.[102]

The Broadcast Content Complaints Committee is an independent organization established by the Indian Broadcasting Foundation. The council consists of 13 members, including the retired Supreme Court or High Court judge's as chairman and rest 12 other members. TV programs received from viewers or other sources (including non-governmental organizations, the Ministry of News and Broadcasting, etc.), and ensure that the programs comply with self-regulatory content rules.

5.3.3 Wider Interpretation of Freedom of Press

The Indian constitution explicitly specifies "freedom of speech and expression" as a Fundamental Right, but these are not absolute rights, and reasonable restrictions may be imposed when and if appropriate.

India, like several other countries, including the United States, does not have a special clause in its Constitution that deals with or guarantees press freedom. The Indian Constitution's authors were well-versed on the United States' First and Fourteenth Amendments. The relevant Supreme Court decisions, despite their best efforts, did not include constitutional protections protecting press freedom.

The term "freedom of speech and expression" is broader and includes all possible ways of expressing opinions, thoughts, beliefs. This expression can be written, printed, photographed, or in other ways, including press.[103]

In Ramesh Thapar v. State of Madras, the Supreme Court of India noted the importance of the right to freedom of speech and expression and quoted the following words:

"Freedom of speech and of the press lay at the foundation of all democratic organizations, for, without free political discussion no public education, so essential for the proper functioning of the processes of popular government, is possible. A freedom of such amplitude might involve risks of abuse. But the framers of the

[102] "Recommendations on Issues relating to entry of certain entities into Broadcasting and Distribution activities." Telecom Regulatory Authority of India. November 12, 2008, available at http://www.trai.gov.in/trai/npIoad/Recofmnendatiom/102/recoml2nov08.pdf
[103] *Id.,* at 20.

constitution may well have neglected with Madison who was the leading spirit in the preparation of the First Amendment of the Federal Constitution, that it is better to leave a few of its noxious branches to their luxuriant growth, than, by pruning them away, to injure the vigour of those yielding the proper fruits".

In Sharma v. Sri krishan,[104] ,it was stated in the judgment that *"The freedom of press, under the Indian Constitution, is not higher than the freedom of an ordinary citizen. It is subject to the same limitations as are imposed by Art. 19(2), and to those limitations only".*

But is to be noted that the restrictions which are to be imposed upon the press should be reasonable. The Supreme court of India highlighted major concepts related to privacy and journalism in famous case of Prabha Dutta v Union of India[105]. In this case journalist requested the court to grant permission to take interview about one of the prisoners in jail but however court did not went into the favour of journalist. Court highlighted about the concept of privacy involved in this matter and a journalist is allowed to take interview of a prisoner in prison only with the consent of the prisoner because privacy of the prisoners are at stake in such cases.

In "R. Rajagopal v. State of Tamil Nadu" ,[106] It was first time in the Indian Judiciary that Supreme Court discussed the right to privacy related to press freedom and ruled that the press has the right to publish a prisoner's autobiography, but only to those extent of information should be used which are available in public domain . However Supreme court clearly underlined that if those facts and details about the prisoners are published that are not available in public domain then that will clearly amount an infringement on privacy of prisoner and thus actionable.

5.4 Social Networking Sites and Privacy Issues

Modern technology has led to the widespread storage of huge amount of data . User profiles and buddy networks are the two fundamental components of most social networking platforms. A user profile is a comprehensive overview of a user's personal information and preferences, including photographs, music, movies, motion graphics, and everything else. The essential lifeblood of social networking sites, on the other

[104] AIR 1959 SC 392.
[105](1982) 1 SCC 1.
[106] (1994) 6 SCC 632.

hand, is friendship networks. They are different from blogs, online magazines, personal websites, and other personal media on the Internet. [107]

Many privacy issues arise when using social networking services. Users' data is allegedly transferred to third parties for commercial, surveillance, or data mining purposes on these sites. Many technologies, like as facial-recognition software, have been implemented on the sites, which can automatically identify people in posted images. Furthermore, such tagging occurs without the consumers' knowledge. Another common practise on these sites is third-party applications' capacity to capture and publish user data without their permission or knowledge. Furthermore, social networking sites frequently employ automated ‘opt-in' privacy measures. It's also been claimed that the sites follow users when they leave social networking sites. The services are also being used for stalking and other forms of illegal tracking of users' physical movements, as well as exposing youngsters to a variety of abuses. Moreover, the users are ill informed and unaware about the processing of their personal information.[108]

The Organization for Economic Cooperation and Development (OECD) created eight principles at the international level: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness principle, individual participation, and accountability principle. As a result, the European Union governs social networking sites using these principles. The Information Technology Act of 2000 governs social networking sites in India. This legislation addresses data protection and privacy concerns. Social networking sites are referred to as "intermediaries" u/s 2(1)(w) of the IT Act of 2000. As a result, all laws and regulations developed under the IT Act of 2000 must be followed by social networking sites.

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.

[107] 4 Melissa L. Rethlefsen MLS, “Social Networking,” Medical Reference Services Quarterly, 26:S1, 117-141, at 120 (2007), available at http://www.tandfonline.com/doi/abs/10.1300/J115v26S01_07#.Uk0CF5HrZjo

[108] Shannon Vallor, "Social Networking and Ethics", in Edward N. Zalta (ed.), The Stanford Encyclopedia of Philosophy (Winter 2012), available at http://plato.stanford.edu/archives/win2012/entries/ethics-social-networking/.

It is concluded that new mediums of expression have brought many challenges in front of us for preserving our right to privacy. The journalists have become stronger than ever by adopting the most sophisticated scientific tools. But at the same time, their responsibilities towards society are also increased. In India, the media is largely self-regulated. The journalists are bound to observe their professional ethics, drafted by the self-regulatory bodies like Press Council of India and Broadcasting Council of India. The legislature is also empowered under the Constitution of India to impose rational limitations on the freedom of media. Similarly, the journalists are always expected to observe individuals' privacy rights while reporting any news. In India, the legislations are insufficient to regulate sting operations. Due to unhealthy completion in the sphere of journalism, the journalists are compelled to report sensational news. For this, they intrude into the private lives of others. For this, senior journalist Paranjoy Guha Thakurta said that The media's ethical standards have been reduced as a result of fierce competition among newspapers and television news channels. He also stressed the importance of a provision for statutory media regulation, which would help to ameliorate the situation. He said that self regulation worked up to some extent only. He stated that corruption among individuals in the media or among media institutions was as old as the media itself. According to him, media was once a part of the solution, but many journalists nowadays were part of the problems. After conducting an inquiry on "paid news" , Mr. Thakurta said that it had gone beyond individual greed and venality undermining the democracy itself. People believed in the Fourth Estate most once, but it presented a sorry state of affairs now as media ethics had become more like oxymoron, an expression with contradictions, he stated. Yet, there was a lot of hope for the future from Indian media and journalists as many good journalists were still around in the profession.[109]

Not surprisingly, public interest may override one's right to privacy. But at the same time, such public interest test is expected to be applied in the fair manner. For this, the journalists should be well trained morally, ethically, and legally. Increasingly, right to speak freely, freedom of association, etc. are part and parcel of right to privacy. Therefore, users' speech and expression should be protected on the social networking

[109] "Competition harming media ethics," available at http://www. The hindu. com/news/national/andhra-pradesh/competition-harming-media-ethics/article38 J 5719. ece

sites. Online users should be protected from arbitrary arrests. More importantly, the social networking sites are bound to protect its users' human rights

Chapter 6

ROLE OF JUDICIARY IN MAKING FUNDAMENTAL RIGHT TO PRIVACY

6.1 Introduction

An essential condition that must exists in peaceful society is the sense of justice among people. In case of a society not having a sense of justice among people cannot be peaceful and that society will be more of a jungle than a society. To express the human approach in a positive way it must be said that Justice is extremely necessary for maintaining peace and security in society and throughout the country.[110]

Earlier, the judges in India we're not inclined towards their function of law-making. This hesitation of judges in exercising this function was due to newly prepared constitution. Although, even before the constitution was enacted courts in India had held legislature statues as ultra vires (beyond power) by exercising their power of judicial review. However, this power was restricted and not used in regular manner. There were no where mention of fundamental rights that means legislative acts and can only be challenged in courts on the ground of lack of authority or power. The ability of courts to judicially review any statute of the legislature or administration extended significantly in every dimension after the Indian Constitution was enacted on January 26, 1949. The role of curator and guardian of fundamental rights has been handed to the court.[111]

Before the coming of decision in Maneka case, the courts were mainly of riches and poor had difficulty in approaching courts. However, after the decision of Maneka Gandhi case the courts were continued to be a rich man courts but gave rise to a new kind of activism where it facilitate the court access to poor. As a result, the court has given normative power to two completely opposing activisms, one of which is functional to fundamental social transformation and the other is dysfunctional.[112]

---

[110] Umeshwar Prasad Verma, Law Legislature and judiciary, 82 (1996).
[111] S.P. Sathe, "Judicial Process: Creativity and Accountability", in K.L. Bhatia (Ed.), judicial Activism and Social change, 90-105, at 91 (1990).
[112] Mohammed Ghode, " The Two Faces of Judicial Activism", in K.L. Bhatia(Ed.), judicial Activism and Social Change, 106-127, at 106(1990).

Starting from the early 1980s, the Supreme Court modified the doctrine of standing and pleading by adding a twist that now even a concerned citizen, public spirited persons, and Ngo's can make a case before the court on behalf of persons not having sufficient means and education or knowledge to challenge the violations of their constitutional rights. As a result late number of applications was filed in the court by various persons or organizations on behalf of persons who were reluctant to go in courts for redress of their grievances. Those applications includes applications for protection of environment. While deciding these cases, the court itself constituted commissions for conducting investigations and court even increased its jurisdiction and remedial power by directing the government institutions to launch various programs and prepare schemes to lessen the effect of alleged violations. By the inclusion of Public Interest Litigation Jurisdiction in the domain of Supreme Court, it acted as a constitution protector and an examining magistrate at the same time. PIL gives a model for the guidance of court to do complete justice by enforcing equal rights given to marginalized society.[113]

Following the introduction of the new field of Public Interest Litigation, the courts established a number of fundamental rights that aren't even included in the Constitution. As a result, the courts can be credited with a vital role in the recognition and development of India's Right to Privacy. The judiciary added new meaning to terms like "personal liberty," "life," and "process established by law to protect people's privacy rights," as well as expanding their scope. The court even recognised the right to privacy of convicts and women in the sphere of life and personal liberty.

Article 21 of the Indian Constitution states:

“No person shall be deprived of his life or personal liberty except according to procedure established by law.”

Article 21 of the Indian Constitution appears to be a universal moral guideline at first glance. On a literal reading, it looks to be a colourless provision. On the surface, it simply states that whatever must be done in accordance with the law's method, but this "procedure set by law" has been understood by the courts to mean that the process must

[113] Burt Neuborne, “The Supreme Court of India”, 1 International Journal of Constitutional Law 416,at 503(2003).

be reasonable, fair, and just. As a result, Article 21 of the Indian Constitution has provided a safe haven for a variety of rights.[114]

The constitutionality of search and seizure from a person against whom a FIR has been filed was challenged in the 1954 case of "M.P Sharma v. Satish Chandra." The key question was whether the search and seizure processes were in violation of Article 19 (1) (f) of the Constitution, which dealt with property rights (prior to the 44th Amendment Act coming into effect), and Article 20 (3), which dealt with the right to self-incrimination.

The judges had to decide whether power of government for search and seizure has any limitations and if this power of government in any way breach the right to privacy.

At the time of the court's decision in this case, the concept of privacy as a right to an individual was unique. The right to privacy is not a constitutionally guaranteed right, according to the majority of the eight-judge court. The bench didn't have a lot of detail. The scope and extent of this right grew with the passage of time.

The majority acknowledge search procedure as a “temporary interference for which statutory recognition was unnecessary". It was recognized as a reasonable restrictions on the freedom of an individual that is constitutional.

The case of " Kharak Singh V. State of UP" was resolved in 1962. The government's act of spying was challenged as a violation of the privacy rights. Due to a lack of evidence, a man named Kharak Singh was discharged from a dacoity case. He was subjected to routine surveillance by the government, which he challenged on the grounds that it infringed on his privacy rights.

The rules and powers mentioned in Uttar Pradesh police regulations includes the secret surveillance of kharak house, uncertain visited at night, officers inquiry, and eye on his movement. Troubled by all this Singh challenged such actions of the authorities and filed a writ petition claiming the violation of his fundamental rights.

In this case, a six-judge constitutional panel reviewed whether the powers granted in the UP police regulations are legal and do not violate the Indian constitution's guarantee of citizen freedoms. The constitution's Article 19 (1) (d) (ability to move freely across

[114] PM Bakshi, The Constitution of India, 54 (2004).

India's territory) and Article 21 (Right to life and personal liberty) were among the rights challenged by Kharak Singh.

The issue that has to be decided by the court was that whether imputed UP police regulations is in violation of citizen fundamental rights..

The main contention of the up police was that the regulations did not violate any of the freedoms mentioned in the constitution and the regulations fall in the ambit of exception or reasonable limitations as mentioned in Article 19(2) in the general public interest that authorizes police to discharge their duties more efficiently and effectively.

At the end in this case the majority ruled that privacy was included in any of the right provided by the constitution to the citizens of India. However, the minority held that right to privacy being a personal right falls with in the ambit of Article 21(right to life and personal liberty), in who's domain many personal rights exists. The regulations allowing authorities for conducting domiciliary visits ruled to be infringement of the constitution.

In the case, the dissenting judge justice subbarao,, said that right to privacy is a one of the crucial right as a fundamental right however it is not expressly given anywhere in the constitution. However, the justice held the rules authorizing for domiciliary visits to be unconstitutional.

6.2 Prisoners' Privacy Rights

By giving new dimensions to the term 'personal liberty' , the courts do recognize prisoners' privacy rights. The cumulative effect of various prisoners' rights like freedom of speech, right to bail, right to live in hygiene conditions, compensation, protection against custodial torture, inhumane treatment, etc. create prisoners' right to privacy.

In its earlier decisions, the Supreme Court had held that prisoners also have right to freedom and speech even though they are in jails.[115] Thereafter, in Charles Sobraj v. Superintendent Central Jail,[116] and Sunil Batra v. Delhi Administration,[117] the Court ruled that prisoners can't be denied their basic fundamental rights of equality or life

[115] State of Maharashtra v. Prabhakar, AIR 1966 SC 424.
[116] AIR 1978 SC 1514.
[117] AIR 1978 SC 1675

and personal liberty. However rights other than those can be denied by considering the nature of the imprisonment. The court further ruled that the prison rules framed for the prisoners can't be in violation of prisoners above mentioned fundamental rights and every prisoner must be treated in accordance with those framed rules. For instance, inhumane torture can't be given to any prisoner while he/she is in a prison. Right to religion is also available to the prisoners. Other rights of prisoner can only be defined till the time he/she is in prison.

The Supreme Court evolved another dimension of right to privacy to prisoners in the case of " Prabha Dutta v Union of India". In this case, the direct issue was not about the right to privacy of prisoners but the court recognized the privacy right indirectly. In the case press authorities asked for the permission of Supreme Court to conduct an interview for different prisoners. The Supreme Court ruled that the press can only interview and photograph prisoners only after obtaining their consent. Journalists have no absolute right as the right to privacy is also available to prisoners detained or confined in jails.[118] Further Supreme Court in the case of "R. Rajagopal v. State of Tamil Nadu" ruled that life story or autobiography of the prisoner (auto shankar) can be published even without obtaining his consent but the publication can only include the information that can be obtained through records available to public. In case they publish anything that is not available in public record they are clearly violating prisoners right to privacy and ultimately they will be liable to be punished according to law. The state has no authority to subject the publication of this to unnecessary restrictions. The court also stated that every citizen has the right to safeguard his or her own privacy, family, marriage, and all other personal affairs. No other person has a right to publish anything about another privacy matters without that other person's consent and if publication is made without his consent on the above stated matter that would amount to violation of that person's right to privacy and the infringer is liable for damages to the person who's rights are infringed.

In the case of Neelabati Bahera v. State of Orissa, a young man was killed after being beaten by police. His mother brought the case, and the Supreme Court awarded her compensation. The Supreme Court ruled that the Supreme Court's power to do comprehensive justice includes the ability to introduce new tools as needed.

[118] Madhavi Goradia Divan, Facets of Media Law, 122 (2006).

In case of "D.K. Basu v. State of West Bengal",[119] the Supreme Court said that death in the custody of authorities is not only inhumane but also crime against humanity and moral conscience in any society where theory of rule of law prevails. The rights guaranteed by Articles 21 and 22 of the Indian Constitution should be safeguarded. Any individual in detention who is exposed to harsh or cruel treatment, whether during interrogation, investigation, or any other action, is infringing on the right granted under Article 21 of the Constitution. If the authorities who are supposed to protect the rights of individuals become law breakers than the faith of people in the justice delivery system would be ruined and people will start taking law in their hands instead of approaching authorities and ultimately that would lead to anarchanism. . Every individual in custody has this vital constitutional right, which is codified in Article 21 of the constitution, unless the legislation specifies otherwise. Reasonable, fair, and just requirements must be met by the procedure. The court went on to say that the phrase "right to life and personal liberty" encompasses not only the right to live, but also the right to live with dignity, as well as the prohibition of torture and degrading treatment by state officials who are entrusted to protect individuals.

Every right comes with a set of restrictions or limits. The right to privacy is not immune to it, is susceptible to constraints, and is not universally available to citizens. In "Peoples' Union for Civil Liberties (PUCL) v. Union of India," the candidate's right to privacy was not violated by disclosing his criminal histories, assets, and obligations to the public. The right to obtain information on a candidate takes precedence over the candidate's right to privacy.

Similarly, in "Mr. K.J. Doraisamy v. The Assistant General Manager," [120] the madras High court that right to secrecy to be maintained by the bank can be undermine by the restriction on the ground of general public interest according to the circumstances.

6.3 Medical Confidentiality and Medical Examination

In the famous case of "Mr. X v. Hospital Z",[121] Supreme Court observed the importance of secrecy to be maintained between a doctor and his patients. The facts were, the appellant was HIV-positive who was going to married to a girl and the fact

[119] AIR 1997 SC 610.
[120] Writ Petition no.17761 of 2006. Available at http://indiankanoon.org/doc/251249/.
[121] AIR 1999 SC 495. Available at http://indiankanoon.org/doc/382721/.

of appellant being HIV positive is known to the doctor. Later doctor informed this fact to the girl's family and they called off the marriage. They contention of the appellant was that the respondent owe a duty towards him to maintain the confidentiality of the disease and they made a breach of that duty and therefore they are liable to pay damages. The court acknowledge that right to privacy is a crucial human right that can come into play by any contract or existence of certain relationship. The court observed that the relation of doctor and patient is to maintain the confidentiality. So in case of doctor patients relationship the disclosure of true facts by the doctor may result into violation of right to privacy of the patient. The court further observed that disclosure of true facts about patient that is in the prevention of public tranquility from being disturbed can be done.

The Supreme Court also stated that the right to privacy does not exist in its entirety, and that reasonable constraints can be imposed on the basis of disorder, crime prevention, health, morality, and other freedoms. So in the present case if the doctor would not informed the family of the girl about the disease of the patient the girl would have been infected of the disease that could cost her life. So, in present case the doctor can't be held liable for breaching confidentiality as it was done for saving the life of the girl.

Further the court held that section 269 and 270 of IPC, 1860 cast an duty on person suffering from communicable disease or impotency, must not marry to anyone as thier marriage will have the effect of transferring the disease to their spouse. The communicable perennial disease is mentioned as a ground of divorce in every personal law.

However, in its later decision of "Mr. X v. Hospital Z", the Supreme Court said that there was no need for this Court in Mr. X v. Hospital Z, to go beyond the facts in issue, particularly when the proper hearing was not given to the relevant parties like Non-Government Organizations representing HIV or AIDS infected persons, etc. As the Court stated, it was unnecessary to go in detail to determine rights and obligations in such circumstances or whether such persons suffering from HIV or AIDS are entitled to be married or not or whether such persons would commit an offence under law if they get married or whether such right to marry is suspended during the period of illness. Therefore, the Court in above mentioned case, held that there is no

infringement of any right of the appellant and the court further clarified that if infected spouse obtains the consent of the healthy spouse and healthy spouse is willing to be married then there will be nothing that can stop them from being married.

Also in divorce proceedings court can compel a person to subject himself to medical test to determine the truthness of an alleged fact. In the case of "Sharda vs Dharampal", Supreme court said that on the petition for divorce on the ground of impotency, schizophrenia the medical examination of the person against whom processing are going plays an significant role in determining the reality. Court held privacy right is not absolute and any matrimonial court may direct a person to subject himself to a medical test and such order shall be valid and not to be considered as violative of Article 21. However court directed that such a power can't be used in routine manner and in every case but only in those case where prima face satisfaction is there by the material produced before them.[122]

6.4 Women's Right to Privacy

The domain of right to personal liberty contains certain women's rights like the right not to ask for women mensuration, presumption of chastity of women, and right not to order paternity test to establish the legitimacy of child unless prima facie is established. The Supreme Court of India in "Bodhisatwa Goutam v. Subhra Chakraborty"[123],observed that rape destroy the mental state of a victim and left her in trauma that is difficult to bear. Rape is not only a crime but also a lack of fundamental right to life and liberty.

In the case of State of Maharashtra v. Madhukar N. Mardikar,[124] the Supreme Court ruled that right to privacy is available to all women including a women of easy virtue and anyone who infringe that right has to face consequences. Anyone who tries to invade in her privacy the women has a right to defend her person and she will be protected under the law even though she causes harm to the offender. Hence, a women of easy virtue can give evidence and her evidence can not be thrown overboard.

In order to build a good and comfortable relationship between women and society focus should be gather on Gender Equality. By 'Gender Equality' means that women must

[122] AIR 2003 SC 3450. Available at http://indiankanoon.org/doc/!309207/.
[123] AIR 1996 SC 922.
[124] AIR 1991 SC 207.

be given secure environment in society where non- discrimination prevails. It can only happen in such a protective space that a women would attain personal freedom. In the case of Vishaka v. State of Rajasthan, [125] the Supreme Court issued detailed guidelines for the guard of the women at a work. The facts of the case were that a women was gang raped at her workplace in a village at Rajasthan. This act was clear violation of gender parity and right to life and liberty. This violates the articles 15, 14 and 21 of the Constitution. It is a fundamental human right to provide a secure environment at workplace. The court further observed that gender equality is seriously violated when women is subjected to gender related offences like sexual harrasment at work place. The court further expanded the definition of sexual harrasment by including "unwelcome sexually determined behavior as physical contacts and advance, sexually coloured remarks, showing pornography and sexual demands, whether by words or actions." These acts are humiliating and may cause mental and physical problems. When a women has sufficient grounds that she will be subjected to disadvantage and gets an hostile environment then that would be discriminatory. Therefore, the court further directed that effective procedures for complaints and compensation should be provided.

In 2010 another case of Alarmelu Mangai v. The Secretary to the Government of Tamil Nadu, [126] the Madras High Court observed that the mental trauma faced by the victim by the act of violating right to privacy can not be compensated by monetary means but the respondents cannot be go unpunished for violating the rights of the petitioner. So, respondents are liable to pay compensation to the petitioner.

In the case of Neera Mathur v. LIC, Life Insurance Corporation put up the questions to her employee named Neera Mathur to tell him about her mensuration and it's cycles and pregnancies and abortions. to uncover the information regarding her cycles of mensuration, conceptions and pregnancies and abortions. The Supreme court find that questions embarrassing, and asked the LIC to refrain from asking such questions and delete the questions from their interview process. In the case of "Surjit Singh Thind v. Kawaljit Kaur," the Punjab and Haryana High Court ruled that putting a woman to a test to determine her virginity is a blatant breach of her right to privacy under Article 21 of the Indian Constitution. In this case, the woman filed a court application for

[125] AIR 1997 SC 3011.
[126] W.P.NO.14781 of 2004. Available at http://www.indiankanoon.org/doc/1841762/.

divorce from her husband, saying that he is absolutely impotent. The husband requested a virginity test for his wife. The High Court dismissed the application, stating that granting it would constitute a major violation of the right to private.

6.5 Personal Decisions Over One's Own Body

The case of "Naz Foundation v. Government of NCT of Delhi" is one of the most important decisions of the Delhi High Court that led to the growth of personal liberty. In this case, the Naz foundation, an NGO, filed a Public Interest Litigation (PIL) challenging the constitutionality of section 377 of the Indian Penal Code, which deals with unnatural offences. This section was challenged to the extent it provide punishment for consensual sex between adult persons Consensual sexual actions between adults were also made illegal under section 377 of the IPC, which was challenged under articles 14, 15, 19, and 21 of the constitution. The petitioner argued that section 377 should only apply to penile non-vaginal sex with minors and penile non-vaginal sex without consent or against the will of a person.

After hearing both sides, the High Court found that section 377 of the IPC infringes on Articles 21, 14 and 15 of the constitution to the degree that it pertains to consenting sexual acts between both parties. The section will, however, continue to apply to all other activities, such as sexual acts between adults of the same sex without their consent or against their will, and sexual intercourse with minors of the same sex. A person under the age of 18 is considered an adult in the IPC.

Now the trend has changed and Supreme Court is more inclined towards protecting individual liberty. In case of S. Khusboo v. Kanniammal[127] the court ruled that live in relationship is a right of decisional privacy. The court approach towards preventing the honor killing in the country shows the inclination of courts toward right of people to choose their partners freely.[128]

The Supreme Court ruled in Srivastava and Others v. Chandigarh Administration that a woman has the right to refuse or accept procreation. Women have the right to refuse to engage in sexual activity or take any form of contraception. All of these rights are protected by the words "personal liberty" in Article 21 of the constitution. Furthermore,

[127] (2010) 5 SCC 600.
[128] Bhagwan Dass v. State (NCT ofDelhi), (2011) 6 SCC 396.

the court concluded that while women have the right to choose whether or not to continue a pregnancy, the state has the right to protect the life of the child, which implies that abortion can only be performed with the court's approval under certain circumstances.

As a result, the Medical Termination of Pregnancy Act of 1971 imposes reasonable constraints on termination and specifies the grounds for terminating reproductive rights.

One of the important question that came up for consideration by the court was that whether a person has right to die with his own consent? The first case on this question was P. Rathinam v. Union of India, [129] where Supreme court held that section 309 of IPC violates Article 21 and is in violation of the constitution. The provision was declared cruel and inhumane. Court further said that the act of suicide is not against any morality, public order and even has no harmful effect on community as a whole.

The Supreme Court's bigger bench later overruled the P. Rathiram decision in Smt. Gian Kaur vs. State of Punjab, stating that the right to life in Article 21 does not include the freedom to die. The right to life encompasses the right to live in dignity and the right to die in dignity, but the right to die in dignity does not include the right to die with one's own consent or with one's own hands, according to the court.

Further in Aruna Ramchandra Shanbaug v. Union of India,[130] in this case the SC allowed to death of a women who is in persistent vegetative state in a hospital on the application of her family and staff friends of the hospital. The court legalized passive euthanasia in this case and direct the government to make a law on this. Supreme court also said that High Court is empowered under article 226 to order on the application filed for the above mentioned purpose. The court specified a proper procedure for applying to the court for permission. Such an application must be authorised by the medical officer and doctors must be consulted by the courts before giving any permission for it. The CJ of high court is bound to make a bench of at least 2 judges whenever an application of this kind is made to the court. The High court is obliged to

[129] AIR 1994 SC 1844.
[130] Writ Petition (Criminal) No. 115 of 2009. Decided on 7 March, 2011, available at http://indiankanoon.org/doc/235821/.

give it's decision at the earliest by recording specific reasons of granting or rejecting such an application.

In last case till date on this issue that had set the controversy at rest was Common Cause v. Union of India, In this case the court came up with the concept of " living will" that means a person can make a will and specify in the will that in case of his condition being deteriorated to such an extent that death would only be an appropriate solution, authorize his near relative or family member to give consent on his behalf for causing his death. The court further give detailed guidelines for obtaining and making of the application to the court. Living will can be made at the time when the person is on hospital bed.

6.6 Mental Privacy

Psychological surveillance consists of those scientific and technological that are used to obtain information from a person that he is keeping a secret and that is necessary to obtain for any purpose.[131]

The Polygraph test, also known as 'lie detection' test, was developed as an instrument to aid police in the detection of crime. The theory behind the polygraph is that lying causes distinctive and measurable physiological reactions in a person who knows that he is not telling the truth. The polygraph operator asks questions in a special pattern while testing the subject's heart and pulse rate, relative blood pressure, breathing, and perspiration rate. Bodily changes are recorded by pens on graph paper, producing "squiggles" resembling those on an electrocardiogram or seismograph. By interpreting these records, a trained polygrapher is supposed to be able to identify untrue responses to critical questions. [132]

Personality test is basically to know of a person's fitness for any employment on the basis of its personality. In addition to emotions, attitudes, propensities, and level of personal adjustment, personality tests also measure subject's attitude towards sexual, political, religious, and family matters. The issue of privacy obviously raised by both

[131] Alan F. Westin, Privacy and Freedom, 133 (1970).
[132] *Ibid.*

polygraphing and personality testing is whether probing of a person inner process through machines or these test is not violative of any right of that person.[133]

Further there are cases when a surveillance may result into voyeurism. Sometimes the person taking polygraphic test may ask some uncomfortable question to a women giving the test. It can be done to satisfy his lust for it. Luke this, sometimes while tapping a persons talking it may happen to hear the personal conversations of persons and inform about it to their knowns.

No doubts technology has made a huge growth over the years. There are techniques that can even see our minds. Functional magnetic resonance imaging (FMRI) technology can make us aware about the perception, emotion, memory and movement. People are trying to be used in investigating process like polygraph tests. But this test must be examined by court whether it violates the fundamental right to privacy of a person.[134] This FMRI can help government to barge into our memory and get any information they want to see even incriminating one. If this would come into use than that would amount to serious violation of various fundamental rights given by the constitution.[135]

Further it was informed by various neuroscientists that various intelligence agencies and military would be using these technology to barge into a person's mind and get any information they want. This was a serious violation and a need had arisen to talk about the mental privacy of a person. Otherwise that would lead to violation of a person rights. For example if a person has claimed that he is not a terrorist but after the test is conducted it is shown that he is a terrorist that would lead to anarchy.[136]

In Selvi v. State of Karnataka, the Supreme Court overturned its position, declaring that the use of these technologies violates fundamental rights and invoking the Right to Privacy. The Supreme Court further ruled that using these methods without the subject's agreement would be a violation of his or her right to mental privacy. If

---

[133] *Id.,* at 134

[134] Mara Boundy, Note, The Government Can Read Your Mind: Can the Constitution Stop It?, 63 HASTINGS L.J. 1 627, 1628 . Available at http://www.harvard-jlpp.com/wp-content/nploads/2013/04/36 2 653 Shen.pdf.

[135] *Id.,* at 1644.

[136] *Ibid.*

accepted without the subject's consent, forcible intrusion can have a negative influence on the subject's mental and physical health.[137]

The Court further expressed it's concern on the possibility of torture and unnecessary harassment to the subject. The court even reprimand the authorities who has leaked the recording of such tests in media or press. This is more of a worrisome procedure as it's video exposure in public would lead to unnecessary stigma attached to that person even before the case is decided by the court.

It can be seen by the conduct of supreme court that SC is expanding the extent of right to privacy. Judiciary inclination towards privacy has removed the social taboo to a great extent. Further this right can't be infringed by private as well as a government official. These are various evolving issue that must be solved by the Indian Courts as the legislations are inadequate to deal with those issues in effective manner.

6.7 Aadhaar and Right to Privacy

Supreme court in a most famous and important judgement finally held that aadhar is valid and doesn't violate constitution when a person of his willingness provide a biometric data. But the SC restricted the use of aadhar in KYC authentication to the private companies. Further Supreme Court allowed the use of aadhar for the purposes like PAN and ITR filing.

The supreme court held the above in judgement of the case named K.S Puttaswamy v. Union of India and provided detailed guidelines for the issues of it. Some of the important points from the judgement are given below:

- When the case was decided the then CJI Deepak Mishra ruled and made aadhar mandatory for filing of Income Tax Returns and also for obtaining PAN number.
- The coirt also held that aadhar must not be required for the purpose of admission in any school nor it be necessary for student appearing in exams of CBSE, NEET and UGC.

[137] *Id.,* at 492.

- Aadhar is mandatory to avail Welfare schemes that are launched by the government for the betterment of the people. It is also made mandatory if individual has to get benefited from the government schemes and subsidies .
- While giving judgment the Indian Apex court found Section 57 of the Act in contradiction with the provisions of the Constitution and thus struck it.
- While delivering the judgement, the Supreme Court went one step further and declared section 57 of the Aadhaar Act unconstitutional. By taking this step, the Supreme Court ensured that no private body or firm can now ask its employees for their Aadhaar numbers.

CHAPTER 7

CONCLUSION AND SUGGESTIONS

It has been observed that when a person is under surveillance, their privacy is always violated. In today's technological world, government surveillance capabilities are becoming stronger than ever. Since after the Mumbai attack in 2011, people have proved that the government's supervision of power is reasonable. It tells about the people's beliefs and confidence in government data collection programs; however, misuse and excessive use of own material for illegal drives Surveillance technology breaks the balance amid privacy, information disclosure and surveillance.[138]

The huge impact of surveillance on human life cant be overlooked, because if surveillance does not give a person the necessary space for action and thinking, he will face some schizophrenic consequences. In fact, privacy is absolutely necessary for a society to work efficiently. Only those who adhere to the ideal of perfection can sail through a high degree of vigilance. However, this is not the case of men in ordinary society. In addition, a person has the right to reveal the secrets of his soul or personality. But forcibly revealing those memories and personality parts that he thinks belong to individuals is tantamount to infringing on a person's psychological confidentiality.

The government is increasingly collecting a large amount of personal data that violates freedom of association, freedom of speech, anonymity. This leds to the huge amount of fear in common people and even can't talk freely due the fear that they might get suspected by the government and then prosecuted. This containment is the central goal of Big Brother Orwell, although it is certainly not suppressed like Big Brother. It lessens the power of contradiction and deteriorates the strength 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,*

[138] Daniel J. Solove, Nothing to Hide, 2.

psychological, and data surveillance technologies, has alarmed the society to show their concern towards privacy rights". [139]

Almost all private sectors are increasingly using technology and software to create their personalised databases where they use to strore a huge bulk of users data .These databases contain information about many variables for many people, and useful correlations can be found. The value lies in the information it contains in the form of potential customers of the company. Today's computers can combine large data sets into a database that can be used to retrieve commercially useful information. Therefore, the commercialization of information and the ability of computers to manipulate information and data have become potential threats to privacy of every user on the web.

The growing use of social media networks has exacerbated concerns about user privacy. It raises concerns regarding data storage and data sharing with other commercial companies.

Following are some important findings:

- In India, right to privacy has been developed in a very limited sense only.
- 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.
- 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.
- The law enforcement agencies have got extensive powers to access online users' personal information.

[139] Alan F. Westin, "Social and Political Dimensions of Privacy", Journal of Social Sciences, Vol. 59, No. 2, 431-453 at 436. Available at http://onlinelibrary.wiley.com/doi/10.1111/1540-4560.00072/pdf.

- 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.
- Public and private agencies have increased its modes of surveillance.
- Majority of people are totally unaware about their data privacy. They hardly know about how their individual information is being processed by the public and private interventions.

Suggestions

Privacy is regarded as "Room to Grow ", freedom from outside intrusion, and liberty to explore and carry out experimental schemes in science, art, work, entertainment and life. One can enjoy such degree of freedom in their private space that they can Interact with others without thinking about if it is allowed or unaccountable. Since privacy is so crucial, it should be protected at any cost. The first step that needs to be taken to safeguard privacy breach is the privacy education. School and Universities should introduce curriculum where whole concept about privacy Infringement and the means to secure oneself should be taught.

If ordinary people (through real education and social examples) believe that privacy is free, their privacy should be respected, .

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. Some suggestions are:

- 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.
- 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 modem patterns of society should definitely be protected from every public criticism.

The continuous broadcasting of provocative headlines against the accused persons while the substance 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. Some suggestions are:

- 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.
- 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.

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 rational limitations on the freedom of speech and expression.

It is submitted that people are nowadays getting fascinated with the concept of online social media. They use to share material and communicate with their friends and strangers on the social networking sites like Facebook, 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. 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.

- 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 organize a user's privacy situations using only a minor amount of energy from the user.
- Privacy policies, like all agreements, should be clear and easy to follow, so that users 1 have a firm grasp on what they are signing-up to.
- 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. The 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.

The study discovered that excessive surveillance has major physical and psychological consequences after analysing main and secondary evidence. Excessive use of surveillance techniques by both public and private bodies has increased the likelihood of a violation of an individual's privacy rights, such as freedom of speech and expression, freedom of movement, freedom of association, freedom of religion, personal autonomy, right to life and liberty, and so on.

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.

There needs to be strong awareness among the common people regarding their data on the web. User should be aware as to for what they are extending their the permission to use their data .

It is becoming increasingly important to comprehensively investigate failure modes prior to the adoption of technologies such as biometric identity cards, in order to anticipate difficulties and how to address them. Furthermore, both the public and commercial sectors should implement mechanisms for installing privacy-enhancing technologies and framing privacy effect assessments. 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. Not only do the naked machines detect contraband, metal, or plastics hidden beneath clothing, but they also reveal disturbing photographs of the naked person. There is also concern that stored or captured photographs would be misused. As a result, the naked machine poses a threat to people's 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 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.

Most CCTV cameras are used illegally or unregulated. For example, outsiders can easily access CCTV recordings and use a videographer to view the recordings as needed. In addition, people install cameras in their shops, restaurants, hotels, etc. Without complying with privacy laws and the government guidelines regarding privacy.

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

- The use of surveillance technologies such as a camera should be used for a specific purpose that has a legitimate purpose and is necessary to meet established emergency needs.
- When using a surveillance camera system, one must consider its impact on personnel and their privacy, and check regularly to ensure that its use is reasonable.
- • The use of surveillance system such as camera should be as transparent as possible, including designated contact points for information and complaints.
- • Before using a surveillance camera system, clear rules, guidelines, and procedures must be established and communicated to all those who need to follow them.
- The stored images and information should not exceed those necessary for the purpose specified by the surveillance camera system, and these images and information should be deleted after the purpose is achieved.
- Access to stored images and information should be restricted, and clear rules should be established to specify who has access and the purpose for which access is granted; data collected through surveillance technologies should be accessed on only those situations there there is involvement of law enforcement.

Researcher extends a crucial suggestion that camera controllers should have cultural, ethical, legal and technical backgrounds, they should understand people's personal

rights, and that the entire CCTV should not have any technical faults. This means that the system must be protected from unauthorized access. No one can copy pictures, recordings, or any other information from the system.

Privacy mainly affects people, and have the authority to decide about extent to which they decide to share their thoughts, feelings, and private lives. In addition, the private sphere may change from time to time, or it may vary from society to society. Local, cultural, and other social factors inevitably influence data protection regulations. Compensation for privacy intrusions caused by unauthorised government involvement, as well as consideration of cultural, sociological, and philosophical traditions Because India has a diverse culture, sociology, and philosophies, privacy is an important aspect of enhancing the development of India's data protection legislation. Various aspects of the issue.

It is recommended that India's upcoming " privacy Act" also develop a system to be jointly supervised by a self-regulatory organization (SRO) and its affiliates to remedy data breaches. The law should impose the most severe penalties for violations of confidentiality regulations. The privacy law should also provide a group of exceptions to RTP. The structure should allow people to resolve their complaints through alternative dispute resolution (ADR) mechanisms, data protection officers, or courts to provide quick relief. The parliament and legislature are accountable to the parliament.

BIBLIOGRAPHY

BOOKS

- Allen, Anita. Uneasy Access: Privacy for Women in a Free Society. Totowa, NJ: Rowman and Littlefield, (1988).
- Bakshi, P.M. The Constitution of India. Delhi: Universal Law Publishing, (2004).
- Blackstone, William. Commentaries on the Laws of England. 1st Edition, 4 Vols., London: Oxford, 1765-69, reprinted (1966).
- Chander, Shailja. Justice V. R. Krishna Iyer on Fundamental Rights and Directive Principles. New Delhi: Deep and Deep Publications, Reprint Edition, (2003).
- Denning, Lord. The Due Process of Law. New Delhi: Aditya Books Private Limited, Indian Reprint, (1993).
- Divan, Madhavi G. Facets of Media Law. Lucknow: Eastern Book Co., First Edition, (2006).
- Universal Law Publishing House, Reprint, (2010).
- Massey, I.P. Administrative Law. Lucknow: Eastern Book Depot, Seventh Edition, (2008).
- Sawant, P.B. Mass Media in Contemporary Society. New Delhi: Capital Foundation Society, (1998).

ARTICLES

- "A comprehensive approach on personal data protection in the European Union," 609 final, 1-19.
- "Authorities and Responsibilities of the Chief Privacy Officer," available at http://www.dhs.gov/chief-privacy-officers-authorities-and-responsibilities
- "DNA, Forensics, and the Law," Genetics and Public Policy Center, 1717 Massachusetts Ave. NW • Suite 530 'Washington, DC 20036 *202.663.5971,availableathttp://www.dnapolicy.org/images/issuebriefpdfs /DNA, %20Forensics,%20and%20the%20 Law%201ssue%20Brief.pdf
- "Medical Record Privacy" available at http://epic.org/privacy/medical

- "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," final,1-54,availableat http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:PDF
- "Social Networking Sites," available at http://epic.org/privacy/socialnet/
- "Surveillance Camera Code of Practice," available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/Jile/204775/Su rveillance_Camera_Code_of_Practice_WEB.pdf
- Bok, Sissela Secrets: On the Ethics of Concealment and Revelation, 10-11(1982). Cited in Raymond Wacks (Rev.), "Secrets: On the Ethics of Concealment and Revelation by Sissela Bok," The Modern Law Review, Vol. 50, No. 1 (Jan., 1987), pp. 125-128 at 126 available at http://www.jstor.org/stable/1095871
- Kupfer, Joseph "Privacy, Autonomy, and Self-Concept," American Philosophical Quarterly, Vol. 24, No. 1 (Jan., 1987), 81-89 available at http://www.jstor.org/stable/20014176
- Miller, Jeremy M. "Dignity as a new Framework, Replacing the Right to Privacy" , in Thomas Jefferson Law Review, 30:1, 1-52, available at http://ssrn.com/abstract=1127986
- MLS, Melissa L. Rethlefsen. "Social Networking," Medical Reference Services Quarterly, 26:S 1, 117-141
- Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems July, 1973. Available at http://epic.org/privacy/hewl973report/
- Warren, Samuel D. and Brandeis, Louis D. "The Right to Privacy" , Flarvard Law Review, Vol. 4, No. 5 (Dec. 15, 1890), 193-220. Available at http://www.jstor.org/stable/1321160 Waters, Nigel "Rethinking Information Privacy-A Third Way in Data Protection?" , 6 Privacy Law & Policy Reporter 121

- Westin, Alan F. “Social and Political Dimensions of Privacy” , Journal of Social Sciences, Vol. 59, No. 2, 431-453, (2003), available at http://onlinelibrary.wiley.eom/doi/10.l 111/1540-4560.00072/pdf.

NEWSPAPERS

- The Hindu
- The Times of India
- Indian Express

REPORTERS

- All India Reporter
- Supreme Court Cases