

SIGNIFICANCE OF PRIVACY IN DIGITAL ERA



Dissertation submitted to

National Law University and Judicial Academy, Assam

in partial fulfillment for award of the degree of

MASTER OF LAWS

Supervised by:

Prof. (Dr.) J. S. Patil

Professor of Law

Submitted by:

Prakhar Puranik

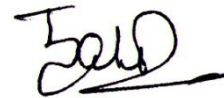
SM0219021

National Law University and Judicial Academy, Assam

August 2020

CERTIFICATE

This is to certify that Mr. PRAKHAR PURANIK has completed his Dissertation titled “SIGNIFICANCE OF PRIVACY IN DIGITAL ERA” under my supervision for the partial award of the degree of MASTER OF LAWS ONE YEAR LL.M DEGREE PROGRAMME.



Prof. (Dr.) J. S. Patil

Professor of Law

National Law University
and Judicial Academy, Assam

Date: August 17, 2020

DECLARATION

I, PRAKHAR PURANIK, do hereby declare that the Dissertation titled “SIGNIFICANCE OF PRIVACY IN DIGITAL ERA” submitted by me for the partial award of the degree of MASTER OF LAWS ONE YEAR LL.M DEGREE PROGRAMME of National Law University, Assam is a bona fide work and has not been submitted, either in part or full anywhere else for any purpose, academic or otherwise.

Date: August 16, 2020



PRAKHAR PURANIK

National Law University
and Judicial Academy, Assam

PREFACE

'Data is the new oil'

The right to privacy is recently recognized as a fundamental right by the Supreme Court. As such it put a duty on the state to protect the welfare of its subjects and protect their rights. The right to privacy is discussed in detail starting with the history in ancient Hindu and Muslim religious texts and how the principles underlying privacy used to prevail in the ancient era. The concept of privacy has developed and evolved over the time along with other legal and technical principles to enter into the modern era. The privacy as a concept is coined by Cooley as a tortuous act and was further discussed by Warren and Brandeis and further the jurists and academicians moved the right through the centuries to today's world. The right of privacy was read with other rights of the individual and it did not emerge as an individual right overnight. This right was first observed as an implied right under the right to liberty. Initially the issues pertaining to the privacy are found in the personal familial rights, liberty rights and property rights. But later with time, they extended further to the areas of technology, security, data protection among others.

To be precise, the privacy which is sought over the internet is known as internet privacy. The concept of Internet privacy came into light with the exceeding usage of internet. In the past decade, internet has just started with the World Wide Web database and now it is spreading very rapidly without any control. The privacy over the internet is mainly about the data what we store in the internet or enter in the internet. The space in internet is like the galaxy, very vast and without any ends to it. This has made the things more complicated as the data we enter in the internet be it pictures, writing, audio, video etc., they have the ability to reach the borders and continents within seconds. Such an unbridled power of the internet is to be curtailed. Nevertheless, the power is so wide to be truncated all over the world. Each country made laws in this regard to protect the data that is entered online or which is collected by the government or the companies. The companies derive their power and money from the data of the individuals only and they will not be ready to act fairly unless they are restricted by the laws of that country. The internet privacy is the subset of the privacy laws. They are also bound by the other freedoms such as the freedom of speech and expression, freedom of assembly, right to life, right to education, and right

to religion of a person. Everything about a person which he doesn't want to be known to the public or any others can be considered as privacy. It has its roots from the natural laws and as such the right to privacy can be said as an inherent right though it is not available directly as a right in itself but was exercised under other major rights such as the right to life, personal liberty, freedom of speech, educational rights, minority rights, religious freedom etc. now that the right has a separate status for itself, this right can be exercised directly and there came new classifications under this right. The concept of digital privacy comes into picture with the exercise of the power by the government and other non-state actors who deploy technologies to track the users, using of blocking and filtering techniques, surveillance mechanisms, data mining, data profiling and other allied mechanism to track the data and use the data for other purposes or send it to third parties who segregate these collected data and then sell it to their customers as per their preference. In India, we have just entered the phase of recognizing right to privacy as a part and parcel of the fundamental rights. We are still naïve in bringing up new statutes or legislative changes to the old statutes and for a concept like internet privacy which falls under the subset of privacy and we do not have any particular law for the online privacy. In India we still do not have a law or inadequate laws relating to internet privacy and data protection.

ACKNOWLEDGEMENT

With profound sentiments of gratitude, I acknowledge the guidance, suggestion and encouragement given by my supervisor Prof. (Dr.) J. S. Patil because of whom I was able to complete the task of writing this Dissertation successfully. I am also grateful to other faculty members for their timely guidance and relevant knowledge regarding various aspects relating to this topic. Also, it is my duty to thank the library staff, who has warmly facilitated the task by providing various books & journals, leading to successful completion of the task.

Prakhar Puranik

UID: SM0219021

LLM

National Law University
and Judicial Academy, Assam

TABLE OF CASES

INDIAN CASES

A.K. Gopalan v. State of Madras

Govind v. State of Madhya Pradesh

K.S Puttaswamy v. Union of India

Kharak Singh v. State of Uttar Pradesh

Maneka Gandhi v. Union of India

MP Sharma v. Satish Chandra

People's Union for Civil Liberties v. Union of India

R. Rajagopal v. State of Tamil Nadu

Selvi and others v. State of Karnataka and others

Suresh Kumar Koushal v NAZ foundation

Unique Identification Authority of India and another v. Central Bureau of Investigation

U.K. CASES

A v B Inc

Associated Newspapers Limited v His Royal Highness the Prince of Wales

Campbell v MGN

CB, Sultan Mohammed v The Queen

Costello-Roberts v United Kingdom

Douglas v Hello! Ltd.

Entick v Carrington

PJS v News Group Newspapers Ltd.

R v Director of Serious Fraud Office, ex parte Smith

RE v The United Kingdom

S and Marper v United Kingdom

Peter Semayne v Richard Gresham

Tude v. Priester

Wilkes v. Wood

Wilkinson v. Downton

U.S. CASES

Boyd v. United States

Griswold v. Connecticut

Katz v. United States

Olmstead v United States

Ontario v. Quon

Roe v. Wade

Wolf v. Colorado

OTHER COUNTRIES

Artavia Murillo ET AL. (“In Vitro Fertilization”) v Costa Rica

Escher et al v Brazil

Lavigne v. Canada (Office of the Commissioner of Official Languages)

Niemietz v Germany

NM and Others v Smith and Others

R v Spencer

Roman Zakharov v Russia

Uzun v Germany

LIST OF STATUTES

INDIAN STATUTES

Aadhar Act, 2016

Banker's Book Evidence Act, 1891

Census Act, 1948

Income Tax Act, 1961

Indian Easement Act, 1882

Indian Post Office Act, 1898

Indian Wireless Telegraphy Act, 1933

Indian Works and Defense Act, 1903

Information Technology Act, 2000

Press Council's Act of 1978

Road Transport Corporation Act, 1950

Telegraph Act, 1885

The Cantonment Act, 1924

The Code of Criminal Procedure, 1973

The Constitution of India, 1950

The Indian Penal Code, 1860

The Indian Post Act, 1898

The National Waterways Act, 1982

The Personal Data Protection Bill, 2019

The Slum Areas (Improvement and Clearance) Act, 1956

Unlawful Activities Prevention Act, 1967

U.K. STATUTES

Bill of Rights, 1689

Human Rights Act, 1998

Justices of the Peace Act, 1361

U.S. STATUTES

Fair Credit Reporting Act, 1970

Freedom of Information Act, 1966

Privacy Act, 1974

The Constitution of the United States, 1789

OTHER INTERNATIONAL INSTRUMENTS

Charter of Fundamental Rights of the European Union, 2000

European Convention on Human Rights, 1953

General Data Protection Rules, 2018

International Covenant on Civil and Political Rights, 1976

Personal Information Protection and Electronic Documents Act, 2007

The Constitution of the Republic of South Africa, 1996

United Nations Declaration of Human Rights, 1948

TABLE OF ABBREVIATIONS

1.	AIR	All India Reporter
2.	Anr	Another
3.	CFREU	Charter of Fundamental Rights of the European Union
4.	Ch	Chapter
5.	Cl.	Clause
6.	CONST.	Constitution
7.	Corpn.	Corporation
8.	CS (OS)	Civil Suit – Original Side
9.	Del.	Delhi
10.	Del. L. Rev.	Delhi Law Review
11.	DLT	Delhi Law Times
12.	ECHR	European Convention on Human Rights
13.	Ed.	Edition

14.	EU	European Union
15.	GDPR	General Data Protection Regulation
16.	GPS	Global Positioning System
17.	Harv. L. Rev.	Harvard Law Review
18.	I.A	Interlocutory Application
19.	I.C.L.J	International & Comparative Law Journal
20.	ICCPR	International Covenant on Civil and Political Rights
21.	Id.	Ibidem
22.	IP	Internet Provider
23.	ISP	Internet Service Provider
24.	IT	Information Technology
25.	KYC	Know Your Customer
26.	LAN	Local Area Network
27.	LGBT	Lesbian, Gay, Bisexual, Transgender
28.	Ltd.	Limited

29.	Mad.	Madras
30.	MEITY	Ministry of Electronics and Information Technology
31.	Nag.	Nagpur
32.	OA	Original Application
33.	Ors.	Others
34.	Ors.	Others
35.	OUP	Oxford University Press
36.	PDP	Personal Data Protection
37.	PIL	Public Interest Litigation
38.	PRS	Policy Research Studies, India
39.	Pvt.	Private
40.	Retd.	Retired
41.	SC	Supreme Court
42.	SCC	Supreme Court Cases
43.	TRAI	Telecom Regulatory Authority of India

44.	TSP	Telecom Service Provider
45.	UDHR	Universal Declaration of Human Rights
46.	UGC	University Grants Commission
47.	U.K	United Kingdom
48.	UN	United Nations
49.	UNHRC	United Nations Human Rights Committee
50.	U.S	United States
51.	v.	Versus
52.	Vol.	Volume
53.	W.P (C)	Writ Petition (Civil)
54.	Yale J.L & Tech.	Yale Journal of Law and Technology

CONTENTS

• CHAPTER 1 – INTRODUCTION.....	1
- Aim.....	5
- Statement of Problem.....	5
- Research Objectives	6
- Scope and Limitations.....	6
- Literature Review	6
- Hypotheses	9
- Research Methodology.....	10
- Research Design	10
• CHAPTER 2 - DEVELOPMENT OF THE RIGHT TO PRIVACY.....	12
- Origin of Privacy and its Jurisprudence	12
- Evolution of the Right to Privacy	19
• CHAPTER 3 - LEGAL AND JUDICIAL PERSPECTIVE OF THE RIGHT TO PRIVACY.....	30
- Contemporary Law in India	30
- Judicial Viewpoint	35
• CHAPTER 4 - COMPARATIVE ANALYSIS OF RIGHT TO PRIVACY IN DIFFERENT COUNTRIES	42
- Privacy in United Kingdom	42
- Privacy in United States	47
- Privacy in European Union.....	51
- International Instruments	59
- Other Countries	61
• CHAPTER 5 - DIGITAL PRIVACY IN MODERN WORLD.....	67
- Communication Privacy	67
- Information Privacy.....	70
- Individual Privacy and Security of State	76
• CHAPTER 6 - CONCLUSION AND SUGGESTIONS.....	81
• BIBLIOGRAPHY.....	xv

CHAPTER I

INTRODUCTION

There are wide definitions of privacy which are broad and are according to its perspective and different situations. In many countries, the concept of privacy is connected with data protection. The facets data protection includes privacy as a tool of a trustworthy relationship between entities associated with giving and collecting the data which includes wide personal information of individuals. Apart from this notion, right to privacy can also be interpreted in a way where it can be said that up to what extent the society can interrupt into the life of an individual and his day-to-day behavior.

According to Black's Law Dictionary, right to privacy means '*right to be let alone, the right of a person to be free from any unwarranted interference.*' The predominant presence of state and non-state entities controls the aspects of social existence which stand upon the freedom of the individual. The legal rights extended from the right to life to the rights in property including tangible and intangible. Thus in this manner the legal rights broadened and as of now legal rights included the right to life which impliedly has right to enjoy the life of a person, right to be and let alone and to an extent to includes the right to be protected from the attempts of causing injury or hurt etc. thereupon emerged the rights wherein the sound, smoke, dust are considered offensive and the concept of nuisance thus developed. A little later, the rights damaging the reputation of the person by way of libel or slander came through. Then travelled to the person's profession, occupation etc. wherein the right to trade and professions emerged which subsequently included the rights of trademarks, copyright, patent infringements. All these rights came from the wake of a person's right to life and liberty and in some or other all these are interconnected to the right to equality, liberty and freedoms. We have the same concept of golden triangle in the Indian constitution which includes the articles 14, 19 and 21.

Justice Thomas Cooley has observed that the law of privacy has the same meaning as the right to be let alone.¹ Professor Edward Shils explained that '*privacy is zero*

¹ Cooley Thomas, A Treatise on the Law of Torts, Callaghan, pp. 29, (1888).

*relationship between two or more persons in the sense that there is no interaction or communication between them, if they so choose.*²

The right to privacy is an elementary human right which is mentioned under the United Nations Universal Declaration of Human Rights,³ the International Covenant on Civil and Political Rights⁴ and by many other international instruments. Right to privacy is a facet of human dignity and also relates to essential rights such as freedom of association and the freedom of speech. It has become one of the pertinent human rights issues of the modern age. Almost every country in the world recognizes the right of privacy implicitly or expressly in their respective constitutions.

Privacy is a state of the individual where a human being has full control over the disallowed intrusion by any person into his or her life. It is true that man is a social animal however he has complete command over his personal existence which cannot be disturbed by anyone without his permission. Right to privacy has justified the need of being left alone.⁵ Right to privacy basically includes the right not to violate the personal space and communications of individuals. Little time ago, South Africa has included the 'right to access' and 'control the personal information of a person'⁶ as a part of the right to privacy into its legislations including the constitution.⁷

There is an ongoing discussion on the special status to be given to the privacy rights in many countries including India. Structural and organizational frameworks have also been analyzed to protect the data of individuals. Such changes are proposed by the legislations which shall be binding on the business organizations.

In the countries like the United States, India, Ireland etc. the right to privacy is not expressly mentioned in their constitutions. However, because of the ruling of their courts this right is recognized as a part of other provisions. The countries who are a signatory to the international instruments like the International Covenant on Civil and Political Rights or the European Convention on Human Rights have inculcated the

² Edward Shils, *Privacy: Its Constitution and Vicissitudes*, Law and Contemporary Problems, pp. 281-306, (1966).

³ Universal Declaration of Human Rights, Article 12, UN General Assembly, 217 A (III), (10 December 1948).

⁴ International Covenant on Civil and Political Rights, Article 17, United Nations, Treaty Series, vol. 999, p. 171, (16 December 1966).

⁵ Rana P.K., *Right to Privacy in Indian Perspective*, International Journal of Law, pp. 07, (2016).

⁶ Protection of Personal Information Act, 2013, Section 14, pp. 32.

⁷ Constitution of the Republic of South Africa, Act 108 of 1996, Section 14, Section 32, pp. 7.

right of privacy into their legislations. The laws concerning the protection of individual privacy started developing in early 1970's.⁸ At present, many countries are still developing the right related to privacy or are yet to develop one for the protection of privacy of an individual.

If we refer to the history of privacy, the basic idea behind the origin of this concept was to protect the manuscripts including art, writings and personal creations. In earlier era the ambit of privacy was not limited only to theft and physical exploitation of property but also against the publication of such property in any form. Therefore, in order to develop and add more into this law many scholars and jurists were of the opinion that the right to be left alone must be read within the law of privacy in order to tackle rapid and continuous changes in technology and with a view that the individual privacy of a person is under constant threat.

With respect to India, there is a stern demand of legislation for the reason that the evolution of information technology has given entities new unrestricted powers by which they can easily gather, store and share private information of individuals. Furthermore, new developments in medical research and care, telecommunications, advanced transportation systems and financial transfers have dramatically increased the extent of knowledge generated by each individual. Computers linked together by high speed networks with advanced processing systems can create comprehensive dossiers on any individual without the necessity for one central system. New technologies developed by the defence industry are spreading into enforcement, civilian agencies, and personal companies.

Digital privacy is another aspect of the right to privacy. It comes into picture when a person, organisation or a state contravenes with the personal data and space of an individual by the use of internet and the devices connected through it. The meaning and data shared willingly by person may differ from person to person in digital space.

There are two aspects of privacy. It can be defined in negative sense and can also be defined in positive sense. The negative aspect to privacy protects the intrinsic identity of a person such as sexual orientation, political and religious beliefs etc. It also protects an individual from the unwanted interference from the government

⁸ German Federal Data Protection Act of 1977, Federal Law Gazette.

instruments and also private actors. Basically, it is the aspect which protects the personal thoughts and beliefs of a person's private life. However, the positive aspect puts an obligation on the part of the state to enact laws to protect the individual identity of a person and eradicating hindrances in their lives which would infringe their privacy.⁹

There is a tendency where negative things tends to grow in a more rapid manner than there positive acts. Similar is the case in the negative and positive rights of privacy. There are arguments where it is said that privacy concerns more about the personal and social rights of an individual. However, we must also know that in this technology driven world the facets of digital privacy are also becoming a pertinent part to be addressed by the state. If we observe closely, the technological advances are also important because they only make our lives better. However, on the other hand privacy of individuals must be taken care of when these advances are made. The need of privacy right is felt more when it is violated. The discussions about privacy have become the need of the hour since with the digital growing world it is one of the most vulnerable rights guaranteed to the individual. There is no doubt about the fact that as we move technologically forward, protection of privacy will get hampered. Also, with the adaptations of new government policies like E-governance, the collection, storage, use and sharing of biometric data has increased. There is always a risk of data leakage from these gigantic databases. Cyber threats are also one of the major problems created by hackers which hampers with the data protection of individuals.

The right to Privacy is an interest with several proportions which also includes the privacy of personal data in internet dominion, known as the 'internet privacy' or 'online privacy'. Internet privacy is the privacy and security level of personal data published via the Internet. It is a broad term and refers to a variety of factors, techniques and technologies which are used to protect sensitive and private data, communications, and preferences. Internet privacy and anonymity are vital to users, especially in this modern tech era. Internet privacy is cause for concern for any user planning to make an online purchase, visit a social networking site, participate in online games or attend forums. If a password is compromised and revealed, a victim's identity may be fraudulently used or stolen. Internet privacy is a subset of data

⁹ Anna Jonsson Cornell, Right to Privacy, Max Planck Encyclopaedia of Comparative Constitutional Law, (2015).

privacy and is necessary to preserve and protect any personal information in the internet domain, collected by any organization, from being accessed by a third party. Further, it is a part of Information Technology that helps an individual or an organization determine what data within a system can be shared with others and which should be restricted. The essence of privacy of personal data is that the individuals can legitimately claim that data about themselves should not be automatically available to other individuals and organisations and that, where the data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use. Such data must be within the controllable limits of the individual whose data is in question and that it shall be used with the consent of the person. Thus, every individual has the desire to control, or at least significantly influence, the handling of data about themselves. There are opposing interests too; but protection is a process of finding appropriate balance between privacy and these multiple competing interests. Internet privacy is perhaps one of the most important personal rights being violated in the realm of liberty without the person himself being aware of such violations.

1.1 AIM

The right to privacy is mentioned under many international instruments and in the constitutions of many countries. This research endeavours to study the pertinence of privacy in modern world particularly in digital era where privacy violations are drastically reported.

1.2 STATEMENT OF PROBLEM

Right to Privacy is now a well recognised and an essential right in the modern age. Therefore, it is also pertinent to take necessary measures to protect such a right. In this age, the privacy right violations have touched a monumental level and these violations are reported on a daily basis. The government and the business entities are accused of gross privacy violations. However, it is also important for the governments to maintain law and order and protect the security of the state and therefore, access to the data of individuals becomes necessary. This research studies how digital world compromises with the privacy of individuals and whether the present laws of India are efficient to protect the right to privacy of individuals.

1.3 RESEARCH OBJECTIVES

The objectives of this research are:

- A. To study the different facets of the right to privacy.
- B. To provide a comparative analysis of different countries about how the law of privacy is guaranteed across nations.
- C. To study how privacy affects digital world and vice versa.

1.4 SCOPE AND LIMITATIONS

The study provides the different aspects of privacy in the modern world starting from its origin, evolution and development. The scope of this research is limited particularly to the concept of digital privacy is studied in detail and critically analysed with the prevalent laws of India to analyse the effect of digital procedures with the privacy of a person. To understand the evolution of the right to privacy, judicial decisions of different countries are also referred. The study is also compared with the laws of different countries such as United States, United Kingdom, South Africa, Brazil, Canada and the countries of European Union.

1.5 LITERATURE REVIEW

Payton TM and Claypoole T, *Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights, and Protecting Your Family* (First paperback edition, Rowman & Littlefield, 2015) – The authors assert that maintaining our privacy is important for our freedom to live the life as we like and it is important to protect our constitutional rights. Even the laws of the United States of America do not stretch far enough to protect us. Every law of any country protecting privacy have flaws and that it is the individual who ought to protect themselves. The author says that the individual should help themselves understand the privacy and know the laws, latest technologies and keep themselves updated to avoid intrusion of privacy. The book also describes the technologies which put us at maximum risk and how they intrude our daily life. The book ends with the regulations and legislations of the United States and the steps to be taken by the legislators and the society to protect their own constitutional rights.

Rakesh Chandra, *Right to Privacy in India with Reference to Information Technology Era*, (YS Books International, 2017) - In this book the author has extensively mentioned the importance of human rights vis-à-vis the mechanism to balance these rights. The book covers the contemporary law in with comparison to different countries with respect to the law of privacy. The author has also mentioned about the checks and balances that a right comes with. The book also covers the technological purview and how it hinders with the privacy of individuals. Besides this, the book also covers that what measures the government must adopt while sharing and collecting the personal information of people and the aspects like data theft, illegal data mining etc. should be covered by a data protection law when it comes into picture.

Ronald J. Krotoszynski Jr, *Privacy Revisited: A Global Perspective on the Right to Be Left Alone* (Paperback Edition, OUP USA, 2018) - The author has given many meanings of privacy and compared them with the definitions given under various jurisdictions of countries. In this book, the author has given reasons as to why right to privacy is a facet of the dignity of an individual. The book has mentioned the objectives that the state must meet while enacting a data protection law or framing the rules and guidelines to protect the autonomy of a person. The book provides a detailed study about substantive and procedural framework of privacy, dignity and freedom of press. Lastly, the book mentions that the law of personal dignity of an individual or law protecting the freedom of speech comes into conflict many a times and in such a case it is important to maintain the balance between the two because both rights have their own protections in their respective spheres.

Gaurav K. Roy, *Cyber Security and Digital Privacy: A Universal Approach*, (Highbrow Scribes Publications, 2020) - This book takes the help of case studies to make us understand how to secure the digital appliances like mobile phones, computers, and networks etc., which store our important data. The author has explained the concepts of digital privacy in a very basic terminology. This book studies the theoretical as well as practical aspects of data breach and also enlists the problems we have to face whilst we deal in cyberspace.

Ajay Kumar Verma, R.K Dubey, *Data Protection and Privacy Implementation: India Perspective*, (Independently Published, 2019) - The book provides an extensive research about the modern data protection rules and regulations in different regimes in

simple terminology. The book has studied the Personal Data Protection Bill of India in a detailed manner and has provided a comparative analysis of the bill with the General Data Protection Rules of European Union and the California Consumer Protection Act of the United States. Apart from this, the book provides a comprehensive study of the privacy laws and regulations in many countries. The book also gives an idea about what needs to be done to protect data when it gets transferred from one country to another and what should be the role of a data protection authority when it comes to the redressal mechanism including penalties and compensation.

Javid Ahmad Dar, *Privacy & Data Protection Laws in India, USA & European Union*, (Walnut Publication, 2019) - This book focuses on to give an understanding of data protection laws with a view of growing commercial transactions in developing world, The book provides a study of various data protection regimes as researchers are regularly required to know the laws of different areas. This book provides the study about the evolution of the right to privacy in India and how the data is protected from time to time. The book endeavours to present a consolidate information on the matter of privacy law. The book also provides an analysis of the data protection laws in India, USA & European Union.

Brian Kernighan, *Understanding the Digital World – What You Need to Know about Computers, the Internet, Privacy, and Security*, (Princeton University Press, 2017) – The author of this book explains about the basics of a computer and information about software, hardware and the role of internet in modern era. The book explains in detail about the functioning of a computer, types of software, computer programming and how the existence of network connections affect the security of data present in a computer system. The book also points out the privacy measures one should take while browsing the internet. The book mentions about how the organisations collected important data such as political views, economic data, and social status of a person through internet. The author has also made a study about the limitations of internet in digital age and how communication privacy is compromised when an individual performs calling and texting via internet and how it affects our daily lives.

Louis Brandeis, Samuel Warren, *The Right to Privacy*, (Harvard Law Review 1890) – This paper is one of the famous researches concerning the privacy of a person. The authors have studies the different origins of the privacy law starting from the common

law countries. Further, the authors have defined many meanings of privacy from the doctrine of right to life and the right to be let alone. The paper also studies the privacy from the aspect of a tort law where the authors have covered the law of slander and libel with respect to privacy. The paper also defines the individual privacy and how it is so pertinent to the existence of a human being. The authors have also compared privacy with the property law where they asserted that the protection of property is the part of right to privacy. The property can be tangible or intangible. Therefore, the authors have covered the intellectual property within the scope of right to privacy.

Buddhadeb Halder, *Privacy in India in the Age of Big Data*, (Digital Empowerment Foundation, 2017) – the author in this paper has mentioned the issues related to privacy of consumers and individuals in India while they enter into a business transaction. The study also covers the use of biometric data and personal information by government agencies and its instrumentalities such as Aadhar Act, 2016 and DNA profiling law etc.

Suneeth Katarki, Namita Viswanath and Nikita Hemmige, *Digital Business in India: Overview*, (Indus Law, 2018) – the authors have attempted to give an idea that where the data goes of the parties which are carrying out business transactions through electronic medium, whether the data is protected sufficiently according to the prevailing data laws in India. Further, the paper also covers the aspect that whether the contemporary law in India with respect to data protection is efficient to protect the privacy. Also, this study had mentioned about the different laws of India which addresses digital business transactions.

1.6 HYPOTHESES

- Digital age hinders the notions of privacy and privacy can be compromised for social security.
- Indian legislative and judicial administration is efficient in dealing with the subject matters concerning to the right to privacy.

1.7 RESEARCH METHODOLOGY

The research methodology of this study is carried by doctrinal method to find out the facts and situations at ground level related to the topic of the research. The methodology adopted in the preparation of the research report is mainly based on secondary sources. The study is carried out by exploring various sources such as books, journals, newspaper articles, online sources, research articles, and statutes, which are available relating to the concerned study. Different research studies and academic lectures had also been critically studied and analysed to study the importance of the right to privacy in tech savvy world. Furthermore, various legal precedents have been studied of India and other countries and are mentioned in the research which concerns the developmental, judicial and legal position of the right to privacy in India and a comparative analysis is made with laws of different countries such as United States, United Kingdom, South Africa, Brazil, Canada and the countries of European Union etc., to study the origins of privacy and to understand the prevalent law relating to privacy in these countries.

1.8 RESEARCH DESIGN

This research is divided into six chapters:

The Chapter I titled “Introduction” deals with the introduction of the research topic. It includes the statement of the problem, aim, objectives, scope and limitations, literature review, research questions, research methodology and research design.

The Chapter II, “Development of the Right to Privacy” will be focusing upon the evolution and growth of the right to privacy in India and the world.

The Chapter III titled “Legal and Judicial Perspective of the Right to Privacy” will be focusing on the contemporary laws and judicial decisions that concern the right to privacy.

The Chapter IV titled “Comparative Analysis of Right to Privacy in Different Countries” will be focusing on the study of the law relating to the right to privacy in different countries and how those laws are different from the prevalent laws in Indian subcontinent.

The Chapter V titled “Digital Privacy in Modern World” will be focusing on the concept of digital privacy in a critical manner. This chapter also studies the concept of digital privacy in contemporary world.

The Chapter V is followed by Conclusion and Suggestions which mentions the concluding remarks relating to the significance of privacy in digital world and thereafter, certain suggestions are being made.

CHAPTER II

DEVELOPMENT OF THE RIGHT TO PRIVACY

- Origin of Privacy and its Jurisprudence

The history of privacy begins with the origin of human beings since human dignity is the intrinsic part of the existence of human beings and privacy is the part of human dignity. The traces of history shows that privacy has always being present in the lives of the people from earlier era. It was a part of social norms and behavior. *Dharmashastra*, the ancient Indian law, comprises of the idea of privacy. There were many ancient Indian rules, norms and laws which are also in the form of extensive commentaries which give the origins of privacy. Therefore, it is important to study the ancient laws relating to privacy and how the law further developed.

The *Dharmashastras* of historical India and their commentaries expounded the legal guidelines of privacy in Indians subcontinent. The kings had been certain to uphold Dharma and to recognize the privacy of the individuals. Further, in topics of spiritual and religious pursuits, interference or disturbances of any type become prohibited. Similar become the case with the Vedas. *Rigveda* truly mounted the priority and awareness of privacy in the historical Indian society with the subsequent verse:

य आस्ते यश्च चरति यश्च पश्यति नो जनः।

तेषां सं हन्मो अक्षाणि यथेदं हर्म्य तथा।।

(One must construct such residence which may also maintain and shield the inmates in all seasons and be comfortable. The persons passing by won't see the inmates and nor the inmates see them.)¹⁰

Historical evidences show that the privacy of the people was an existent social norm in each civilization. *Manusmriti* proves the superiority of guidelines respecting the privacy of people in ancient Indian society. It mentioned that a man or a woman must

¹⁰ Rigveda, Mandal 7, Sukta 55, Hymn 6.

not be disturbed whilst mediating, resting or studying. The following content helps this view:

एकाकी चिन्तयेन्नित्यं विविक्ते हितमात्मनः।

एकाकी चिन्तयानो हि परं श्रेयोऽधिगच्छति।।

(A person should meditate alone and in a lonely place then only he will attain salvation.)¹¹

Kautilya in his *Arthashastra* which he wrote between 321-296 B.C., has recommended a system to make sure that private and internal matter of the kingdom is maintained while ministers of the ruler had consulted.¹² The sole reason of this targeted system prescribed for consulting the ministers is to thrust back feasible leakage or divulgence of the state guidelines and policies and the legacy of that can still be discovered even in present day in the provisions of the Indian Official Secrets Act, 1923.

Right to privacy in India is a combined blend of constitutional, customary and common law rights proliferated over various legal areas. As a customary right, privacy is regarded as an easement forming part of statutory legal right. As a part of constitutional right to life and liberty, privacy is a right which is part of developing modern society which is a facet of right to life. In earlier era, seldom times the right to privacy was compared and understood as a part of tort law however as we progressed it is treated as an independent human right. Many a times, it is discussed that society has delayed in recognizing the right to privacy as a separate legal right because this right has its own pertinence and value. The jurisprudential aspect relating to privacy adds a new dimension to the rights of individual in a modern state.

It is said that the constitution is a living document. It is neither dead nor static. It is an organic document. There were times when the constitution recognized the principles which were customary which were followed from a long period of time. Later the constitution was amended several times when it was known that such customary

¹¹ Hargovind Sastri, *Manusmriti*, pp. 276.

¹² R. Shama Shastri, *Kautila's Arthashastra*, pp. 19, (1961).

practices were no longer needed or did not go according to the test of the constitution. It is true that the customary rules and norms are protected by the constitutional protection and therefore they are practiced. It can also be said that the notions of privacy are not new to the human existence and behavior since they are followed from now long period of time. The philosophical nature of privacy is a reason itself that this right was present from the very earlier time and can be regarded as a modern right.

Many references of privacy can be found in the Holy Bible.¹³ In the Hebrew culture, earlier Greece and ancient China, the protection given to the privacy was well mentioned. The Chorus of Atigone and the Psalmist, thousands of years ago noted that a man is always tensed when another man violates his property and personal belongings. Therefore they regarded this as a shell and said that every human being is shell. The meaning of shell here gave the fundamental basis of privacy. It means that it is a natural behavior of an individual to protect his privacy and when this shell is broken a person gets worried and tensed. Similarly, a person of average intellect always respects the privacy of other person in a society and never discusses private conversation with another person in public. Therefore it can also be said that the right to privacy is a natural right to human behavior and is a facet of natural law.

In Anglo American era, the courts gave judgments on the basis of natural justice and conscience since the positive law was not developed in 1905. The courts and some jurists have argued that privacy must be declared as a part of natural right. The courts have also mentioned that privacy is entitled to be a part of natural right under the purview of natural justice because privacy is based on the instinct of the human nature. Any person instinctively acts on the contraventions to his personal deeds, the deeds which he wants to share with nobody whom he does not want the public to know of. This instinctive behavior of an individual is natural therefore it can be said that privacy is derived from the natural law.

There is another school of thought which endeavors to establish that privacy is a right just like the rights which relate to property, tort, slander or libel. It is important to mention that Justice Douglas of U.S Supreme Court wrote in his judgment in

¹³ Richard Hixson, *Privacy in a Public Society: Human Rights in Conflict*, Oxford University Press, pp. 255 (1987); Barrington Moore, *Privacy: Studies in Social and Cultural History*, M.E. Sharpe, pp. 48, (1984).

Griswold v. Connecticut,¹⁴ that there are many constitutional principle which give protection the privacy of an individual and why create the ‘zones of privacy’. In his point of view, court must have very early directed that the right to privacy is a part of bill of rights. He also said that there are similar writings and jurisprudential aspects which prove that privacy has always been the part of natural law and these writings give inherit the zones of privacy.

The first page of the holy bible gives us an allusive idea about how individuals feel ashamed when their privacy is compromised. It is an incident when Adam and Eve sewed aprons for themselves of fig leaves when they say each other naked after they have seen each other naked after they ate the fruit from the tree of knowledge. It is therefore taught to us that privacy is our intrinsic moral value and we always have an idea of what is right and wrong.

Privacy gives a person space and creates a boundary between the personal life of an individual and public life. It restricts others from entering into the private matters of a person. That is why it is said that privacy is both a negative right and a positive right. Significant traces of privacy can be found in the east and west world countries of the existence of this right. Firstly, the biblical references have been mentioned earlier that establishes the fact that enough respect was given to privacy of persons and secondly, under Hindu manuscripts and commentaries it is well established that how much importance was given to a person while he was in his home meditating or eating or reproducing.

Though there are certain traditional and cultural differences between the east and west world countries, the philosophical ideology concerning privacy remains the same in this matter. It is true that ambit of the right may vary from country to country but there can be no denying of the fact that privacy remains in all domains. However, it must be noted that it is the oriental civilization which led the evolution of modern privacy, especially United States of America. In ancient India, privacy had its place in the lives of the individual. The ancient Indians believed that there is no particular and binding norm to protect the privacy of a person. It can only be said that privacy existed during that time because of available evidence. However, how it was protected, there is no mention of that. The question that how the privacy must be

¹⁴ 381 U.S. 479 (1965).

protected is not even answered by the Romans and Greeks, therefore it can be said that the regulating norms of how the privacy to be protected is rather a modern concept. It is now debated that to what extent the privacy should be protected or when the government can compromise with the privacy.

The discussion on the concept of modern privacy was started in the U.S in 1890 by two lawyers Samuel Warren and Louis Brandeis. In that era, there were ongoing discussions on the freedom of press in the United Kingdom. However, Warren and Brandeis were less interested to compare freedom on press and privacy. They have compared English and American law of torts in this regard. They have made their efforts to study the law of property, law of contract to compare and include the privacy aspect under these laws. They mentioned that it is the duty of the man himself to protect his interest from others and in this sense a man will be able to enjoy his right to be let alone. Warren and Brandeis observed that the personal life of an individual have been so much interfered by others therefore they were of the view that there should be a private personal remedy for the individual and a criminal remedy for violation of his privacy.

Warren and Brandeis opined that there must be a criminal remedy as a form of protection of the privacy. However, they did not deny the fact that there are facets of property law in privacy. They wanted to increase the ambit of liability on the instruments who infringe privacy as they had no objection on the point that privacy right can be covered under libel law but they also had to address the fact that there is agony caused to the individual and what could be the possible remedies for such harm caused. In that time, the law provided mechanism only for the physical harm to the property or personal liberty of an individual. The property included in earlier time was the cattle of a person or his shelter but in modern era this meaning of property has included many things if it is not changed. Therefore, the personal liberty was protected from battery and its other forms. As liberty means freedom from all shackles and later within the meaning of privacy Warren and Brandeis meant that this freedom must not only be physical in nature but also mental i.e. for mind and intellect of a person therefore the scope of right to life was limited to protection of individual from the tortuous acts of battery and trespass. They also mentioned that the common law continues to be evolving to give protections to a person who safeguards his life and property from physical impediments. Thus, right to let alone, becoming a

significant right to human beings, in a way guarantees the right to enjoy life and liberty of an individual.

Dean Prosser of Berkley Law College has mentioned four torts in his book.¹⁵ He argued that firstly, privacy is a composite right and not an independent right. It is a composition of reputation and emotional tranquility of a person and his intangible property. Further, Prosser mentioned that intrusion is another kind of civil wrong which affects privacy. This intrusion means when the physical seclusion of a person is infringed which is expected by him that it would be maintained according to his wish. This wrong is also covered under the law of trespass which is invoked when people discuss privacy violation. Prosser contended for a well drafted privacy legislation to secure personal information of individuals which has now become a subject of concern for every individual. He wanted that legislation to provide a remedy for modern privacy violations such as wire tapping, photo sharing and bugging. According to Dean Prosser, intrusion has three facets. According to him intrusion must:

- a. Be highly offensive to a reasonable person,
- b. Be intentional and
- c. Occur in a place where the plaintiff has a reasonable expectation of privacy.

These elements point towards the individual sovereignty, it means that it is upon the person whether to allow another to enter upon his personal space or not. In short, a person is the master of his own privacy. Privacy is the part of human personality and depends upon the autonomy of an individual which guarantees human dignity to a person and also increases its ambit. To bring respect and integrity to a person is one of the chief objectives of the right to privacy. The personal relations of an individual and a shelter above his head where nobody can see him nor enter inside without his permission are of utmost importance to him. These rights make human behavior better. It protects a person from commercial organizations which always make their way in order to collect his personal information. Subsequently, privacy ensures that the core or inner self of a person stays protected which guarantees him to live in society with respect and dignity. As with the development of technology, digital life and scientific advancements the new threats to the privacy of the individuals have

¹⁵ Prosser, Keeton, On Law of Torts, West Group, pp. 23, (1987).

come up. It is very essential that the forms of invasion of privacy must be identified and proper remedial measures are taken to protect this.

An individual has the right to live his life on his own terms without the state's interference into his personal matters. The idea is that almost all people want to maintain their personal life personal. The state's role is to enact the law to protect this right. The common law mentions that a man treats his house like a castle. This is another aspect of a democratic principle. Kantian philosophy mentions that like physical dignity, spiritual and mental well being of an individual is essential in the similar manner for his overall development. Thus, it can be said that mental and physical dignity of a person is a part of right to life. It is a well established fact that the right to privacy includes personal relations such as family and marriage, reproduction, health, right to prevent others to be watched while performing personal habits, use of contraception etc. The modern privacy covers the aspects such as communication, protection of data etc.

The Bill of Rights of the United States under its constitution contains the provisions which are enacted to protect the personal liberty of a person. The interpretation of these provisions by the courts gives rise to new the rights from these existing rights. The right to privacy is not explicitly mentioned under the constitution. Further, the word privacy is not mentioned at all. It is the judiciary which interpreted the constitution and gave rise to the right of privacy.

The judiciary's approach to include the right of privacy in United States constitution was to assert that the violations to the privacy of its citizens by the government have become rampant and there was no limitation to it. It is to contend that when it comes to invasion of privacy the government leaves no stone unturned while carrying out surveillance, collection of personal data such as biometrics etc. and how much the state must do to protect these invasions since the protection from this invasion of privacy is also the function of government and what measure it takes to protect the privacy of its citizens. When it comes to prevention from a violation, Justice Brandeis of United States once said that:

“from obtaining disclosure in court of what is whispered in the closet, how government is restricted from intrusions into the privacy of the home of the person. How the right of privacy is frequently in conflict with other

claimed liberties and governmental power, and finally, to show how some intrusions of privacy have become accepted as necessary in the interest of public health, safety, morals and the general welfare.”

The fourth amendment of the U.S constitution entails the rights which protect the privacy of individuals. The fourth amendment rights include the right against unreasonable search and seizures, protection from revealing personal documents, papers, conversations etc. Consequently, primary protection of the right to privacy is guaranteed by the constitution itself.

- Evolution of Privacy

The evolution of privacy for what it is today was started from hundreds of years. England’s Justices of the Peace Act of 1361 provided protection against spying or peeping into one’s house and secretly listening to one’s communications without permission.¹⁶

In 1765, British Lord Camden, struck down a warrant to enter a house and seizure of papers. He wrote,

“We can safely say there is no law in this country to justify the defendants in what they have done, if there was, it would destroy all the comforts of society, for papers are often the dearest property any man can have.”¹⁷

Parliamentarian William Pitt wrote,

“The poorest man may in his cottage bid defiance to all the force of the Crown. It may be frail; its roof may shake; the wind may blow through it; the storms may enter; the rain may enter - but the King of England cannot enter; all his forces dare not cross the threshold of the ruined tenement.”¹⁸

Those were the times when the judiciary and the legislature of England have started discussions about the personal liberty of an individual. It was relatively unchallenging to ensure privacy when infringements immediately could be distinguished and arraigned or structured the subject of a civil activity yet it is substantially more

¹⁶ James Michael, *Justices of the Peace Act*, (1361).

¹⁷ *Wilkes v. Wood*, CCP 6 Dec 1763.

¹⁸ William Pitt, Speech on the Excise Bill, (1763).

difficult when we can witness major scientific and technological advancements in modern world, when numerous infringements can't be seen at each time when they are taking place, however their resulting damages may have broad outcomes. While Britain has not many laws explicitly for the protection of privacy, there have been ongoing discussions with regard to a dedicated statute and conversation in academic journals and open discussions for advancing dynamic definition of laws to grant protection from the contravention of privacy of individuals. When the discussion is about the most technologically and economically forward society is considered, in the United States, the courts have proclaimed the presence of privacy rights as part of present rights in the Constitution and the legislation of the country has endorsed a few laws managing explicitly for the protection of privacy issues.

When it comes to the Indian subcontinent, there are numerous ongoing discussions happening in the country with regard to right to privacy after substantial judicial decisions in its favour in recent years. There were prevailing statutes in India which already provided for the protection of privacy of individual. The Indian Penal Code, 1860 is 19th century legislation which provides for the protection of the modesty of women under its section 509.¹⁹ Similarly, Section 26, 164(3) and 165 of Code of Criminal Procedure, 1898 provides for protection of privacy regards of an individual. The Indian Evidence Act, 1872 in its certain sections provide the protection of the privacy interests of an individual. The Indian Evidence Act under Section 122 provides that there is no compulsion to a married person that he must reveal the personal communication with his spouse during the course of their marriage.²⁰

Furthermore, the Banker's Book Evidence Act of 1891 gives protection to a customer from disclosing of the financial transaction details. However, the court may order for an inspection on reasonable grounds under section 6 of the Act. Section 18 of The Indian Easement Act, 1882 provides that the female person in the house have a right to stay in house with seclusion and that no outside person such as neighbour should be able to see them to infringe their privacy. Section 137 of the Income Tax Act, 1961, aims to protect the financial transactions of an assessee. This is to protect the economic interest of an individual. Moreover, Section 15 of the Census Act, 1948

¹⁹ Section 509, IPC specifically makes it a crime to intrude upon the privacy of a woman intending to insult her modesty.

²⁰ This section also creates a disability that no such person shall be permitted to disclose any communications. The marital privacy, to an extent, is thus protected.

provides that the personal details of a person must not be leaked by the hands of the government while or after carrying out the census in the country. These were the statutes which aim to protect the privacy of persons however there are certain legislations which on reasonable grounds can compromise with the personal liberty of people.

Under The Indian Post Act, 1898²¹ the State and Central Governments have the power to intercept postal letters and can open them to check whether the article inside poses threat to public order. However, this power is available when it is provided in writing and only on the occurrence of a public emergency or to maintain public tranquillity. To protect the right to privacy of citizens, the Second Press Commission in India recommended an amendment to the Press Council's Act of 1978 which conferred the power upon the press council to check whether the news agencies, reporters, journalists and newspapers are maintaining the highest standards while disseminating information in public.²²

After the independence, India witnessed many rights being emerge as a part of existing rights which granted the right to clean environment, right to education, etc. Similarly, the right to privacy is a modern right in India while plethora of debates, discussions were carried out while interpreting and understanding the doctrines of due process of law and procedure established by law.

Kazi Syed Karimuddin, the member of the Constituent Assembly, has proposed addition to the clause of the draft Article 14 (now Article 20 of Indian Constitution) which was identical to the fourth amendment of the U.S constitution which guaranteed protection of privacy and provided the right against unreasonable search and seizure. The chief draftsman of the constitution, Dr. B. R. Ambedkar has supported the idea of Kazi Karimuddin however his support was rather limited and reserved and the amendment failed to be incorporated with no right to privacy in the constitution.

²¹ The Indian Post Act, 1898, Section 26.

²² India: Second Press Commission, Volume 1, Controller of Publications, (1982).

The facets of personal liberty were limited at that time therefore the members of the constituent assembly have omitted the significance of privacy and have failed to incorporate the right to support it and provide protection.²³

After adopting its own constitution in 1950, Indian lawmakers did not find a reason to debate on the issue of privacy of individuals and the fundamental rights mentioned under Part III of the constitution did not incorporate the right to privacy. Due to the continuance of common law practices, the Indian judiciary also did not give much significance to the right of privacy. There were cases which are mentioned in upcoming chapters where the discussions of privacy started to happen. However, the courts were of the view that India does not need a privacy law at that time.

Nevertheless, the constitutional provisions were wide enough to interpret that the right to privacy was introduced and became a part of right to life and personal liberty.

As the technology has developed, the privacy of an individual is under greater threat of being compromised. The prevalent laws do not properly address the violation of privacy when an individual is carrying out his business on the internet. After much debates and deliberations, the Information Technology Act, 2000 was enacted in India. The object of the act is to provide a transparent mechanism to the individual in order to get information from the public authority. The act also makes the authorities accountable and this liability is available for the technological platforms to protect the information of individuals on the internet.

The right to life is a well established right under Indian legislative administration. Having its vast scope, the right also protects a person on the ground of health including mental torture. It also safeguards a person from fear of injury and unwanted interference.²⁴

The Indian legal system further ensures that while asking personal information of a person, the consent of an individual is of utmost importance, as and when required to be exercised must be free, revocable and voluntary. The decisional aspect of consent relies upon his 'will' however this part is very subjective in nature. There are many

²³ Constituent Assembly Debates, Vol. VII, pp. 794, (1948-49).

²⁴ INDIA CONST, art 21.

statutes²⁵ which require the consent of the owner or occupier, to be obtained prior to any entry is made into any establishment, building or similar premises.

Freedom of Press has been acclaimed as the cornerstone of modern democratic state. It is often described as fourth estate.²⁶ The press enjoys a prestigious position in democratic countries where constitutions guarantees freedom of press. The freedom, like all other liberties, cannot be absolute and is subjected to restrictions in public interest. Privacy of individual is a right to be protected even from the gaze of the press. Invasion of privacy by press may arise when information about private affairs of a person is published by newspaper. In India, the media culture has drastically changed from what it was at the time of independence. Now, the media persons are adequately paid when it comes to their payment. In the words of Justice Krishna Iyer,

*“Press has the public duty to inform or expose even the private life of public persons, which affects the people's interest. Where a reputed journal devoted to the dissemination of information on public matters or personalities for democratic edification comes with important discoveries bearing on a high functionary's private sexual deviance impacting on his image and activities as a public servant, exposure of such delinquency is the public duty of the Press in a democratic polity.”*²⁷

The freedom of speech and expression and the right to privacy are both complementary to each other. On one hand, freedom of speech grants a person the right of information and on the other hand we have right to privacy, the right which enables a person to remain alone. In certain circumstances, the right to be alone is violating when anyone wants to access information from a person who does not wants to share such information. The fact cannot be denied that how important the privacy of a person is to him but the right of knowledge under the freedom of speech and expression is also of paramount importance as the information many a times is in public interest in a democratic structure of the government.

²⁵ The Indian Works and Defence Act, 1903, Section 4; The Slum Areas (Improvement and Clearance) Act, 1956, Section 27; The Cantonment Act, 1924, Section 247; The National Waterways Act, 1982, Section 10; The Oriental Gas Company Act, 1857, Section 2 and the Road Transport Corporation Act, 1950, Section 42.

²⁶ Lucas A. Power, The Fourth Estate and the Constitution, Berkeley: University of California Press (1991).

²⁷ V.R. Krishna Iyer, Essays on Press Freedom, Capital Foundation Society, (1996).

It is the duty of the court to interpret the constitutional principles, thus to maintain a balance between the fundamental rights. Therefore, a harmony must be construed between the freedom of speech and the right to privacy of a person. The advancement of media in present day times has an extraordinary importance to the development to bring the private existence of a person into the open area, along these lines presenting him to the danger of an intrusion of his space and his protection. To keep the Press as a solid medium that can defend open intrigue it must watch self-oversight with a lot of standards dependent on sound rules that proposal due respect to both the opportunity of articulation and right to privacy.

In such a case, Press Council can assume a significant job by providing legitimate guidelines to print and digital media. The conundrum here is whether all media actors would view such rules with due regard or would they ridicule the standards for making space for trending stories that would expand the course. The problem may be about a thoughtful extent on the off chance that one solicits whether the intention of a news industry is to update people in general or to rather engage to the detriment of profound quality and ethics of media.²⁸

Like the privilege of the sacredness of one's home, the option to maintain this right for correspondence is additionally one of the relevant aspects of the right to privacy. In the typical importance of the term correspondence covers all interchanges between various people by methods of letter exchange. Article 8 of the European Convention on Human Rights alludes to secure the correspondence, not the whole communication all in all. Extensively, the Convention secures the intention to secure all communication methods, whatever their essence is whether it is by phone, electrical, mobile, and wired and so forth. Subsequently, the interference, concealment or revelation of a message sent by these methods for correspondence can give rise to an infringement of Article 8 of the Convention.

Human nature to ensure that his messages are secure is as old as the foundation of spying which is regarded to be one of the earliest professions of the world. Interference of messages and other communications by postal control, surveillance, tapping phones and hacking mechanism is the standard act of modern secret service organizations.

²⁸ R. Rajagopal v. State of Tamil Nadu, 1995 AIR 264.

In the earlier times, since spying was carried out through *Gudha Lekh*, for example foreordained signs and set of operations, and with help of pigeons and spies, it was more likely than not made expounded efforts to crack these messages. *Mudraraksasa*, a Sanskrit epic, composed by *Vishakadutta*, makes reference to the specialty of opening a fixed letter without harming the seal.²⁹ In this manner, as the position stands today, subject to the superseding forces of the State during an open crisis, secrecy of sending messages and information is very much secured in the Indian legal framework in ordinary and general conditions. During a time of changed kinds of correspondence, privacy is unmistakably under a great threat however the legislators have indicated a need to worry on this issue.³⁰ While in across other nations, there are currently a number of laws that have been set up that looks to secure these rights, Indian laws regarding the matter fall a long ways behind.

Privacy of a person has become a much deliberated topic in today's democratic structure of governments. Social orders are portrayed as an important part of refined bureaucratic administrations. Cutting edge innovations in the fields of communication and data frameworks have posed a major need of reforms. A central point of the privacy issue is that no deliberation on an enactment and composed principles guaranteeing privacy, secrecy and fair treatment to the subjects of electronic data. Information banks have been set up at all offices of the Government, business and the military administrations with no genuine information regulatory body whole role is to safeguard the expected effect of individual rights. The privacy issue is even more earnest in view of far reaching utilization of data frameworks to regulate administrations which numerous individuals may consider basic to their prosperity and good stature.

Alongside the estimations of a democratic framework, individuals have continually rising desires as far as health care services, well being, insurance services, loans and credit, family help and other services. Those looking for employments, credit, lodging, government assistance and different administrations must furnish broad data of a specific sort, so as to acquire these advantages. The data further amasses into the documents kept up by different private and open establishments. On the off chance

²⁹ D. S. Trivedi, *Secret Service in Ancient India*, Allied Publishers Pvt. Ltd., (1988).

³⁰ Privacy Act, 1988, Federal Register of Legislation; Data Protection Act, 1988, Law Reform Commission (United Kingdom).

that the realities about an individual are shared without checks and balances with the information and assent that they might have been imparted to other people, there has been no infringement of security of the breach of personal information.³¹

The privacy issue includes different concerns frequently connected with the mental space, however in reality it is not kept in mind for the idea of legislation concerning privacy. Individuals may feel compromised by the presence of enormous and productive data collection frameworks despite the fact that the protection has not really been compromised. They are regularly worried about the continuous threat of information sharing by social researchers, business organisations, assessment surveyors and the organizations that utilize the information.

Technological advancements have permitted the individual a more prominent scope of decision than he has ever wanted previously, one that may additionally even be a befuddling expansive. It is a contention that new issues are getting importance because of exploratory innovation and can be comprehended by the utilization of more innovation in the field of social science. The protection of privacy of a person is an issue in any case, and it will experience the ill effects of being entangled in this discussion. Since innovation is setting down deep roots, the private conversation ought not to concentrate on its attractive quality, but instead on discovering approaches to ensure humanistic qualities and objectives. Given the straightforwardness and speed with which data goes from one association to the next, it could turn into the reason for unfair segregation. Be that as it may, comparatively with expanding legitimate acknowledgment of protection of data, there has built up a structural problem to violate it by various methods up to this time. Information on people is gathered on a monumental level and as handily put away. What is scientifically conceivable will be enacted and implemented.

The cause for protection of data is up to the more broad discussions with respect with the impact of innovation in society. Some contemporary scholars share a sceptical perspective on this relationship and reason that what is in fact achievable is permitted to happen without respect for the possible outcomes.

³¹ Hyman Gross, Privacy - Its Legal Protection, Oceana Publications, (1976).

Professor Arthur R. Miller, distinguishes between four ongoing improvements that identify with the late twentieth century which is in regard for protection of data.³² Gigantic record keeping, dynamic dossiers, unhindered exchange of data starting with one individual then onto the next and sharing directly at many levels. He further expresses that the new theories of data protection doesn't identify with interruption of communication, misappropriation, no proper rules for ensuring the private rights of a person. These things establish that the job of attorneys is limited to get things done under their purview to ask information about the individuals. Be that as it may, record-keeping and information collection gives rise to new and various methods of violating the personal space and time as an ever increasing number of organisations gather increasingly more data about more parts of our lives.

Professor Miller is correct in suggesting that innovation progresses tend inflexibly to limit the faultless zones of privacy. It isn't just the law and Justice administration that has a summary of information on private residents. There is a particular administration for the health and well being of a citizen that administers information to insurance agencies on the medical history of individuals for protection. With the advancement of the computers, it has gotten conceivable to gather, in a split of second to recover and break down huge measures of individual data. Access to this individual information has been extended by the computer's capacity to recover information get to office, institutional, legislative and geographic limits.

It would be false to say that endeavours have not been made to build up some type of guidelines or control in regard of the utilization of information in United Kingdom. In 1961, Lord Mancroft presented a Bill in the House of Lords to shield an individual from any baseless distribution identifying with his exclusive issues of private life and to give him direct legal protection in case of such distribution. Bills concerned principally with electronic data were presented in 1969, and in 1972. During 1969 a private member's bill, the Data Surveillance Bill, was presented in the House of Commons with the point of giving enactment to forestall the attack of privacy through the abuse of computerized data. The Bill didn't become a law however all things considered was included in the coming new recommendations, for example, enlistment of computer based information banks and the obligatory publication of

³² Richard F. Hixon, Privacy in Public Society, Oxford University Press, pp. 183, (1987).

print outs which likely could be encapsulated in a future enactment. Most legal advisors and authorities presumably felt that it is too soon to be certain precisely that governmental arrangements are alluring. However in any case, the Data Surveillance Bill was a significant commitment to begin with the general assessment to the kind of measures that may in the long run be important. Some portion of the data concerning personal information isn't of such a genuine nature. Be that as it may, some sensitive information is important to be protected. At the point when we talk about security of data, we ought to comprehend related idea of privacy and confidentiality moreover.

Since there are some basic highlights between confidentiality and secrecy, it is important to understand that there is a difference between the two. Protection as a human right must be recognized from confidentiality and privacy. Confidentiality is an is a part of a bigger right and keeping in mind that protection is an end in itself, classification is rested, confidentiality is kept up and security of data is regarded. One reason of confidentiality is to cultivate the right of data protection of an individual and the job of classification is to safeguard private life and personal data. In India, confidentiality as a standard is opposed to the special case. There are various explanations behind keeping up confidentiality in governmental administration. Confidentiality is vital in light of a legitimate concern for territorial protection, national security, relations between two nations, criminal law, individual protection and intellectual property and so on.

The governments of modern times gather a great deal of data from its residents about their issues. This data may identify with wellbeing, trade and economic activity, monetary status of a person. This divulgence of data may hurt their dignity and infringe their fundamental freedoms. Be that as it may, now and again even access to this data must be permitted to decide if the government has been regulating the law with unacceptable regards and with an inconsistent hand to offer advantage to the individuals who were not legitimately guilty. However, the data isn't significant for this reason and it is the acknowledged standard of nondisclosure, giving regard to the essential right of privacy of a person. At the point when the individual has provided data intentionally to the administration it might be important to keep the data in secret hands to spare him from constant worry and burden. On the off chance that intentional data or its source is uncovered it might deny the administration for the access of future data.

Data is private when it is endowed to another, in the conviction that it will go no further conditions much of the time emerge in which an individual conveys private realities on the understanding that access to it will be declined to all. Spare the beneficiary or, now and again, to the individuals who have certain interest in knowing about it. There has been an expanded worry in India about the effect of information security laws which is authorized and well executed in different nations.

CHAPTER III

LEGAL AND JUDICIAL PERSPECTIVE OF THE RIGHT TO PRIVACY

- Contemporary Law in India
 - a. Information Technology Act, 2000

The Information Technology Act, 2000 contains provisions regarding the safeguarding of the online privacy³³, online fraud and hacking,³⁴ data protection standards for the corporate bodies,³⁵ monitoring and collecting of online traffic data,³⁶ surveillance, monitoring and decryption of communications³⁷ etc. Going in detail into the provisions of the Information Technology Act, 2000 and the Information Technology (amendment) Act, 2008, there are certain sections which are essential to be discussed in relation to the subject at hand.

The information technology act was enacted with an objective of providing recognition to the transactions that are carried out in online medium, e-commerce transactions and the businesses that arise through the technological medium. As we witness the expansion and growth in technology, the act underwent amendments and also published rules and regulations time to time to come up with the pace of the technology. In the hurried process, there still remained some gaps. From last decade itself, there was a need for the laws relating to the online privacy and data protection in the internet realm. Further, the collection, processing and usage of the data of individuals for the use of government through policies like Aadhar are not efficient at that point of time. There was a push for such laws from a very long time. We have a need to put in laws relating to the internet privacy concerning the freedom of speech and expression. Though the IT act is all about the technology, privacy and protection of data, it is important to discuss with special emphasis to the internet privacy and the freedom of speech and expression. In order to protect the individual privacy of

³³ The Information Technology Act, 2000, No. 21, Parliament of India, pp. 67.

³⁴ The Information Technology Act, 2000, No. 21, Parliament of India, pp. 43.

³⁵ Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data Or Information Rules, (2011).

³⁶ Information Technology (Procedure and Safeguards for Monitoring and Collection Of Traffic Data Or Other Information) Rules, (2009).

³⁷ Information Technology (Procedure and Safeguards for Intercepting, Monitoring, And Decryption) rules, (2009).

citizens, the Information Technology Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules of 2011 were framed.

In general, the information that is disseminated in the internet is dealt by the intermediaries only who host the internet to the users and the content which users post go through the intermediaries. In the Information Technology act, 2000 there is a provision i.e. section 79 in which the intermediaries are held liable for the content for some extent which goes through them. This was amended in the 2008 amendment and the new provision provides a safe harbour to the intermediaries i.e. section 79 of the act exempted the intermediaries from the liability of hosting unlawful content in certain circumstances. The contents of the provisions of section 79 in both IT act, 2000 and IT (amendment) act, 2008 are as follows:

The IT act, 2000 in chapter XII states with a head note ‘network service providers not to be liable in certain cases’ and the provision³⁸ reads (section 79):

“For the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this Act, rules or regulations made there under for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention.

Explanation – for the purposes of this section –

- a) *“network service provider” means an intermediary;*
- b) *“Third party information” means any information dealt with by a network service provider in his capacity as an intermediary;”³⁹*

Section 79 of the amended Information Technology Act (2008) which was added in Chapter XII of the act titled ‘Intermediaries not to be liable in certain cases’⁴⁰ and the section reads as –

³⁸ The Information Technology Act, 2000, No. 21, Parliament of India, pp. 79.

³⁹ Ibid.

⁴⁰ The Information Technology (Amendment) Act, 2008, No. 10, Parliament of India, pp. 79.

“Exemption from liability of intermediary in certain cases:

- 1) *Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.*
- 2) *The provisions of sub-section (1) shall apply if-*
 - a) *the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or*
 - b) *the intermediary does not:*
 - i. *initiate the transmission,*
 - ii. *select the receiver of the transmission, and*
 - iii. *select or modify the information contained in the transmission;*
 - c) *the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.*
- 3) *The provisions of sub-section (1) shall not apply if-*
 - a) *the intermediary has conspired or abetted or aided or induced, whether by threats or promise or authorise in the commission of the unlawful act;*
 - b) *upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource, controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.*

Explanation - For the purpose of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary”⁴¹

Both the texts of the previous act and the amended act speak of the intermediary liability only but the terms are different from that of the IT act, 2000. This amended provision makes it a safe harbour as the intermediary is not made liable if it only

⁴¹ The Information Technology (Amendment) Act, 2008, No. 10, Parliament of India, pp. 79.

facilitates the content but has no knowledge of the same, the intermediary can be directed by the court⁴² to remove such content. In furtherance, there are rules framed subsequent to the act which the intermediary has to follow in order to avail the exemptions under section 79 of the principal act. The term intermediary is defined under section 2(w) of the principal act⁴³ which is also amended under the IT (amendment) Act, 2008 and is defined as:

“‘Intermediary’ with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes.”⁴⁴

b. Data Protection Bill, 2019

The data protection law in India is still in developing phase. Data Protection Bill of 2019 was introduced in late 2019 in the legislature to protect the privacy of individuals and to protect their personal data from sharing and usage by unlawful means. The bill aims to create a mutual understanding and trustworthy relationship between the individual and data collecting entities so that the data of such individual could be processed in a cautious manner in return of the services provided to them by those entities. The bill also ensures that no unauthorised sharing will be done by these data collecting entities. The bill also aims to create an authority (Data Protection Authority) to protect the data of individuals.

The ambit of this bill is quite expansive as it covers majority of businesses in India such as real estate, healthcare services and pharmaceutical companies etc. The scope of this bill is also extended to protect digital processing of data in the sectors like E-commerce, social media and information technology sector. However the small entities like business which collect information on manual basis are covered under the exception under this bill. But, they also have to act in compliance of the bill.

⁴² Shreya Singhal v. Union of India, AIR 2015 SC 1523; Supreme Court read down section 79 to mean the actual knowledge from the direction of a court order or from the appropriate government.

⁴³ The Information Technology (Amendment) Act, 2008, No. 10, Parliament of India, pp. 2.

⁴⁴ Ibid.

The financial services and telecommunication sector are governed under their own respective laws and their regulators have already set certain strict and cogent norms to protect the privacy of individuals and to provide confidentiality to their data.

The Data Protection Bill, 2019 gives directions to the data collecting and data storing entities to obtain consent by the individuals for such measure. The entities must also preserve such evidence where the consent of the individual was received. Under this bill, the individuals can also get access to their data⁴⁵ in one place. Further, they can also make corrections and can even delete their personal data. One of the most pertinent features of this bill is that the consumers can withdraw their consent to collect and store data by the businesses.

Another important feature of this bill is transfer of data. There are certain cases where a person wants to change his place of work or he wants to terminate a particular service provided by a respective business entity and switch to another entity whose service is better than the previous in the idea of the consumer. In such a case he can transfer his data to other business entity. The Data Protection Bill, 2019 makes it compulsory to business entities to make and include organisational changes into their framework to protect the privacy of the individual at each step. This is also called as privacy by design principle. The bill also specifies that the sensitive personal data shall be kept in Indian servers only and such sensitive data must not be transferred from India to any other country. This bill also creates a group, from many data fiduciaries called as significant data fiduciary where the duty of this group is to audit the personal data of individuals and to ensure that data is stored in a fair and responsible manner. The group of significant data fiduciary is also in charge of appointing data protection officers. With respect to the infringement under this bill, the Data Protection Authority has the power to impose fine any business entity who does not act in accordance with the bill. The maximum penalty which the bill specifies is either rupees fifteen crores or four percent of the global turnover of the business, whichever is higher.

In Chapter VIII of the PDP bill which deals with exemptions, sections 35 provides power to the central government to exempt any governmental agency from this act and section 36 also exempts certain provisions from application in processing of

⁴⁵ Sec. 17, Data Protection Bill, 2019, Parliament of India, pp. 11.

personal data. These provisions provide much power to the central government in excluding any government agency and exempting the provisions of the act. Certain provisions are also not applicable to the courts and other law enforcement officers under section 36 of the bill.

The significant changes made to the PDP bill, 2019 from that of the 2018 bill and the draft bill proposed by the committee is that a separate class of intermediaries is made which includes the social media intermediaries who enable the individuals to interact and pass information to one another in the internet realm. This is a welcome change as the data that is exchanged and disseminated under the social media and online media comes under the purview of the PDP bill, 2019. But another change is that the bill gives more power to the central government in exempting governmental agencies from the bill which may hamper the whole idea of bringing the legislation.

- Judicial Viewpoint

The judicial evolution of the right to privacy started in the year 1950 with the infamous case of *A.K. Gopalan v. State of Madras*⁴⁶ where the court was of the opinion that Article 21 only guaranteed procedural due process and the preventive detention legislation under which the petitioner was detained was a valid law and in accordance with the constitution. Even though there are some fundamental rights of the petitioner have been infringed such as the freedom of movement and the right against arbitrary detention mentioned under articles 14 and 19. The rationale that came out of this decision was that Article 14, Article 19 and Article 21 are not in nexus with each other but are separate and independent rights because these rights are also different to one another.

In the case of *MP Sharma v. Satish Chandra*⁴⁷ the court has held that the search of property and seizure of articles does not violate the right against self-incrimination. The court also observed that if the framers of the constitution itself did not intend to inculcate the right guaranteeing privacy to individuals just like the fourth amendment of the US constitution, they have no justification to adjudge this as a fundamental right. Moreover, even the framers of the constitution were not of the view that the

⁴⁶ AIR 1950 SC 27.

⁴⁷ (1954) SCR 1077.

power of search and seizure by the state authorities violate the right to privacy. Therefore there is no question to include the right to privacy in our constitution.

In *Kharak Singh v. State of Uttar Pradesh*⁴⁸ court adjudged that

“the Indian Constitution does not contain a guarantee similar to the Fourth Amendment of the US Constitution, it proceeded to hold that the right of privacy is not a guaranteed right under our Constitution and therefore the attempt to ascertain the movements of an individual which is merely a manner in which privacy is invaded is not an infringement of a fundamental right guaranteed by Part III.”

However, if we refer to the dissenting judgment of Justice Subba Rao, we can observe of an idea that the right to privacy was being given importance. He held that:

“Personal liberty must not exclude the right of a person to sleep which is very essential requirement to the existence of a human being. Every person has a right to get comfortable sleep. Further, if the policemen invade the home of any individual at this odd hour, it will amount the violation of the right to sleep. The essential human needs are a part of personal liberty of a person which helps in overall development of a person. The preamble of the Indian constitution also guarantees to assure the dignity of the individual.”

Justice Subba Rao referred upon the judgment of *Wolf v. Colorado*⁴⁹ which held that,

“The security of one's privacy against arbitrary intrusion by the police is basic to a free society. We have no hesitation in saying that a state was affirmatively to sanction such police incursion into privacy it would run counter to the guarantee of the Fourth Amendment.”

The right to personal liberty includes not only a right to be free from hindrances placed on the movements of a person, but also free from intrusions on his private life. Article 21 grants the right to the individual to be free from restrictions or encroachments. In this view, though the Constitution does not expressly declare the

⁴⁸ (1964) 1 SCR 332.

⁴⁹ 338 U.S. 25.

right to privacy as a fundamental right, such a right is essential to personal liberty of a person. Subsequently, Justice Subba Rao mentioned that the right to privacy is a constitutional principle and an ingredient of personal liberty under Article 21 of the Constitution.

The next landmark case concerning the right to privacy is *Govind v. State of Madhya Pradesh*.⁵⁰ In this case the judgment of the Supreme Court is considered ambiguous because there was no clear cut rule or guideline was mentioned by the court concerning protection of privacy of an individual. However, the court was of the view that the right to privacy is an important right to an individual but the Indian constitution does not contain this right. The court held that:

“There can be no doubt that privacy-dignity claims deserve to be examined with care and to be denied only when an important countervailing interest is shown to be superior. If the Court does find that acclaimed right is entitled to protection as a fundamental privacy right, a law infringing it must satisfy the compelling state interest test. Then the question would be whether a state interest is of such paramount importance as would justify an infringement of the right... Assuming that the fundamental rights explicitly guaranteed to a citizen have penumbral zones and that the right to privacy is itself a fundamental right that fundamental right must be subject to restriction on the basis of compelling public interest.”

In another *locus classicus* case of *Maneka Gandhi v. Union of India*⁵¹, it was established that the constitutional doctrine is that, the expression ‘personal liberty’ in Article 21 covers a variety of rights, some of which ‘*have been raised to the status of distinct fundamental rights*’ and given additional protection under Article 19. The decision in *Maneka* carried the constitutional principle of the over-lapping nature of fundamental rights to its logical conclusion. Non arbitrariness but reasonable principles are the key elements of the guarantee against arbitrary state acts under Article 14 with is also in nexus with Article 21. A law which provides for a

⁵⁰ 1975 AIR 1378.

⁵¹ AIR 1978 SC 597.

compromise of life or personal liberty under Article 21 must lay down not just a procedure which is fair in nature but a procedure which is ‘just, fair and reasonable.’

In the case of *R. Rajagopal v. Union of India*,⁵² the Supreme Court recognized that the right to privacy can be both a tort, a civil wrong whose remedy can result in an actionable claim as well as it can be a fundamental right. The court further held that:

“A citizen has a right to safeguard the privacy of his or her own family, marriage, procreation, motherhood, child-bearing and education among other matters and nobody can publish anything regarding the same unless (i) he or she consents or voluntarily thrusts himself into controversy, (ii) the publication is made using material which is in public records (except for cases of rape, kidnapping and abduction), or (iii) he or she is a public servant and the matter relates to his/her discharge of official duties.”

In *People’s Union for Civil Liberties v. Union of India*,⁵³ the Supreme Court extended the scope of life and personal liberty and mentioned that the communications of an individual comes under the purview of the right to privacy. The Court also laid down the guidelines that form an essential subject for the checks and balances in interception provisions in India, they are:

- i. Interception orders to be issued only by Home Secretaries at both the Central and State governments;*
- ii. Issues such as the necessity of the information and whether it can be acquired by other means to be considered while making the decision to approve interception;*
- iii. The addresses and the persons whose communication has to be intercepted should be specified in the order, which means that the interception order cannot be generic; and*
- iv. Putting a cap of two months on the life of an interception order.*

⁵² AIR 1995 SC 264.

⁵³ AIR 1997 SC 568.

In *Selvi and others v. State of Karnataka and others*,⁵⁴ The Supreme Court accepted the fact that there is a difference between physical privacy and mental privacy. The court held that:

“Indian criminal and evidence law contends that interference with the right to physical and bodily privacy in certain circumstances, but the same cannot be used to compel a person to impart personal knowledge about a relevant fact. This case also establishes the intersection of the right to privacy with Article 20(3) (self-incrimination). An individual's decision to make a statement is the product of a private choice and there should be no scope for any other individual to interfere with such autonomy. Subjecting a person to techniques such as narcoanalysis, polygraph examination and the Brain Electrical Activation Profile (BEAP) test without his or her consent violates the subject's mental privacy.”

Further, in the case of *Suresh Kumar Koushal v NAZ foundation*,⁵⁵ The Supreme Court held that Section 377 of IPC criminalises a consensual sexual act of adults in their personal space is in contravention to Articles 14, 15 and 21 of the Constitution. However the Delhi High Court in the same matter⁵⁶ held that:

“...The sphere of privacy allows persons to develop human relations without interference from the outside community or from the State. The exercise of autonomy enables an individual to attain fulfilment, grow in self-esteem, build relationships of his or her choice and fulfil all legitimate goals that he or she may set. In the Indian Constitution, the right to live with dignity and the right of privacy both are recognised as dimensions of Article 21. The High Court adverted at length to global trends in the protection of privacy – dignity rights of homosexuals, including decisions emanating from the US Supreme Court, the South African Constitutional Court and the European Court of Human Rights. The view of the High Court was that a statutory provision targeting homosexuals as a class violates Article 14, and amounted to a hostile discrimination on the grounds of sexual orientation. However, the SC held that “In its anxiety to

⁵⁴ 2010 (7) SCC 263.

⁵⁵ (2014) 1 SCC 1.

⁵⁶ Naz Foundation v Government of NCT, 2010 Cri. LJ 94.

protect the so-called rights of LGBT persons and to declare that Section 377 IPC violates the right to privacy, autonomy and dignity, the High Court has extensively relied upon the judgments of other jurisdictions. Though these judgments shed considerable light on various aspects of this right and are informative in relation to the plight of sexual minorities, we feel that they cannot be applied blindfolded for deciding the constitutionality of the law enacted by the Indian Legislature.”

In the case of *Unique Identification Authority of India and another v. Central Bureau of Investigation*,⁵⁷ for a reason to investigate a criminal offence, the Central Bureau of Investigation asked for an access to the database of the Unique Identity Authority of India. Conversely, the Supreme Court its interim order held that the data of any person must not be shared by the Unique Identity Authority of India specially the biometric data of persons which is a very essential form of information. If such information goes in the hands of any third party agency without the consent of the concerned person, it would be a gross violation of privacy of an individual.

The case that settled the privacy conundrum that whether this right is a part of life and personal liberty is *K.S Puttaswamy v. Union of India*,⁵⁸ the Supreme Court its landmark judgment held that:

“the right to privacy and the protection of sexual orientation lie at the core of the fundamental rights guaranteed by Articles 14, 15 and 21 of the Constitution. Every individual in society irrespective of social class or economic status is entitled to the intimacy and autonomy which privacy protects. It is privacy as an intrinsic and core feature of life and personal liberty which enables an individual to stand up against a programme of forced sterilization. Then again, it is privacy which is a powerful guarantee if the State were to introduce compulsory drug trials of non-consenting men or women. The sanctity of marriage, the liberty of procreation, the choice of a family life and the dignity of being are matters which concern every individual irrespective of social strata or economic well being. The pursuit of happiness is founded upon autonomy and

⁵⁷ Special Leave Petition to Appeal (Crl) No(s).2524/2014.

⁵⁸ Writ Petition (Civil) No. 494 of 2012.

dignity. Both are essential attributes of privacy which makes no distinction between the birth marks of individuals.”

The central theme is that privacy is an intrinsic part of life, personal liberty and of the freedoms guaranteed by Part III which entitles it to protection as a core of constitutional doctrine. The protection of privacy by the Constitution liberates it, as it were, from the uncertainties of statutory law which, as we have noted, is subject to the range of legislative annulments open to a majoritarian government. Any abridgment must meet the requirements prescribed by Article 21, Article 19 or the relevant freedom. Privacy is a constitutionally protected right which emerges primarily from the guarantee of life and personal liberty in Article 21 of the Constitution. Elements of privacy also arise in varying contexts from the other facets of freedom and dignity recognised and guaranteed by the fundamental rights contained in Part III. Judicial recognition of the existence of a constitutional right of privacy is not an exercise in the nature of amending the Constitution nor is the Court embarking on a constitutional function of that nature which is entrusted to Parliament.

CHAPTER IV
COMPARATIVE ANALYSIS OF RIGHT TO PRIVACY IN DIFFERENT
COUNTRIES

- Privacy in United Kingdom

However, in England there is no established assurance of human rights against the State, the customary law perceives that an individual has certain rights, for example, the freedom to the right to speak freely of discourse, to individual freedom and so forth which the State would secure against attack by different people, to the extent that the ambit of such rights isn't compresses by enactment. There is, be that as it may, no such acknowledgment of any right to privacy in that capacity, despite strong backing by dynamic masterminds, for example, Lord Denning.⁵⁹

The Government of United Kingdom and its Judiciary does, be that as it may, the Human Rights Act, 1998 permits the protection of privacy as a common law right.⁶⁰ The law regarding the matter in the United Kingdom has seen impressive development and change. This change has for the most part been realized by two components: first, the presentation of the Human Rights Act, 1998, which consolidates the European Convention on Human Rights and second, by explicit enactments covering parts of a person's entitlement to protection and the legal development of them.

In the course of this development, the court reviewed existing cases such as *Kaye v. Robertson*⁶¹ where media personnel overlooked a notification disallowing a section to a room where a notable actor was recouping from broad head wounds, and met and interviewed him. An interlocutory order was looked for in the interest of the activity to keep the paper from distributing the article which guaranteed that Kaye had consented to give a select meeting to the paper. There being no right to privacy under English law, the offended party couldn't keep up any suit for protection of privacy. Justice Glidewell observed that there had been a gross intrusion in privacy which

⁵⁹ Denning, *What Next In The Law?*, OUP Oxford pp. 219, (1982).

⁶⁰ Lord Irvine, House of Lords, 24 November 1997, Col. 784.

⁶¹ [1991] FSR 62.

featured a disappointment in English law. Different appointed authorities have concurred with this determination and proposed that an overall right of privacy ought to be perceived. Without such a right of privacy, the case depended on different privileges of activity, for example, criticism, noxious misrepresentation and trespass to the individual, with the expectation that either would assist him with ensuring his protection. In the end, he was allowed an order to limit distribution of the noxious deception. The distribution of the story and some less questionable photos were, be that as it may, permitted depending on the prerequisite that it was not guaranteed that the offended party had given his assent. The solution was unmistakably lacking since it neglected to shield the offended party from protecting his own space and from getting his own conditions far from open glare. The court communicated its powerlessness to ensure the security of the individual and accused the disappointment of custom based law and resolution to ensure this right.

Issues of privacy managed by English law incorporate security of private property, the option not to be mentioned, the option to convey secretly and the option to regard for private life. As an issue of open arrangement, any law identifying with privacy must find some kind of harmony between safeguarding protection and privacy and saving ability to speak freely and access to open data which are pertinent to a modern majority rules system. To be sure the Human Rights Act additionally contains the freedom of speech and expression. Some level of protection is found in English law which is analyzed in the accompanying cases.

In the case of *Wilkinson v. Downton*,⁶² a close relative is found in regard of certain perspectives between right to protection and the law of slander, it is because of the way that in spite of the fact that criticism and defamation are principally concerned about notoriety, in particular, an interest for connection with others. It additionally defends the people in the feeling of respect and sense of pride. In any case, in spite of all that the law of defamation doesn't present assurance against non explanations which would not comprise unfair demonstration of criticism however the equivalent would absolutely add up to unapproved misuse of one's name or propagation of one's decision for business purposes.

⁶² (1887) 2 QB, 57.

The right to privacy was recognized in *Tude v. Priester*⁶³ wherein the court forestalled the respondent who was required to make duplicates of the image having a place with the offended party by keeping duplicates of the image and offering such duplicates to the clients. The court held that the offended party was qualified for get directive just as harms for the violation of their agreement.

There is a classic common law case regarding protection of privacy of a person. It is called the *Semayne's Case*⁶⁴. This case concerns to the access inside a property by the Sheriff of London in order to execute a legally binding writ. The case is well known for the decision of Sir Edward Coke:

“That the house of everyone is to him as his castle and fortress, as well for his defense against injury and violence, as for his repose ...”

In the case of *Entick v Carrington*⁶⁵, Entick's house had been entered in a forcible manner by agents of the government. Lord Camden held that:

“By the laws of England, every invasion of private property, be it ever so minute, is a trespass. No man can set his foot upon my ground without my license, but he is liable to an action, though the damage be nothing; which is proved by every declaration in trespass, where the defendant is called upon to answer for bruising the grass and even treading upon the soil.”

Lord Mustill's observation in *R v Director of Serious Fraud Office, ex parte Smith*⁶⁶ underlines the methodology taken by the customary law to privacy that it perceived protection of a person as a guideline of general nature and that privacy had just been given discrete and explicit regard at custom based law.

There has been a transformation in this approach after the Human Rights Act, 1998 came into force. For the first time, privacy was a part of the British law.⁶⁷ In *Campbell v MGN*⁶⁸, a well-known model was photographed leaving a rehabilitation

⁶³ 19 Q.B.D 1604.

⁶⁴ *Peter Semayne v Richard Gresham*, 77 ER 194.

⁶⁵ (1765) 19 St. Tr. 1029.

⁶⁶ [1993] AC 1.

⁶⁷ The UK Human Rights Act incorporates the rights set out in the European Convention on Human Rights (ECHR) into domestic British law.

⁶⁸ [2004] 2 AC 457.

clinic, following public denials that she was a recovering drug addict. The photographs were published in a publication run by MGN.

She sought damages under the English law through her lawyers to bring a claim for breach of confidence engaging Section 6 of the Human Rights Act. The House of Lords by majority decided in her favor. Lord Hope writing for the majority held that:

“If there is an intrusion in a situation where a person can reasonably expect his privacy to be respected, that intrusion will be capable of giving rise to liability unless the intrusion can be justified... A duty of confidence arises when confidential information comes to the knowledge of a person where he has notice that the information is confidential.”

In *A v B Inc.*⁶⁹ the court held that a duty of confidence will arise whenever a party subject to the duty is in a situation where he either knows or ought to know that the other person can reasonably expect his privacy to be protected. Later, in *Douglas v Hello! Ltd.*⁷⁰ it was held that what the house in *Campbell* was agreed upon was that the knowledge, actual or imputed, that information is private will normally impose on anyone publishing that information the duty to justify what, in the absence of justification, will be a wrongful invasion of privacy.

In *Associated Newspapers Limited v His Royal Highness the Prince of Wales*,⁷¹ an appeal was made against the judgment in respect of the claim of Prince Charles for breach of confidence and infringement of copyright. The case brought about when a newspaper named ‘The Mail on Sunday’ published extracts of a dispatch by the Prince of Wales. The Court held that the information at issue in this case is private information, public disclosure of which constituted an interference with Prince Charles as heir to the throne, Prince Charles is an important public figure. In respect of such persons the public takes an interest in information about them that is relatively trivial. For this reason public disclosure of such information can be particularly intrusive. Prince Charles has a valid claim based on breach of confidence and interference with his Article 8 rights.

⁶⁹ [2003] QB 195

⁷⁰ [2006] QB 125

⁷¹ [2006] EWCA CIV 1776.

In *PJS v News Group Newspapers Ltd.*⁷² Lord Mance, paying emphasis on Article 8 of ECHR held that, “having regard to the nature of the material sought to be published and the identity and financial circumstances of the appellant, that the appellant’s real concern is indeed with the invasion of privacy that would be involved in further disclosure and publication in the English media, and that any award of damages, however assessed, would be an inadequate remedy.”

In the recent case of *CB, Sultan Mohammed v The Queen*,⁷³ where the issue was regarding the retention, inspection, copying and disclosure of electronic data of the complainant for investigation purposes, the court held that:

“Victims do not waive...their right to privacy under article 8 of the ECHR, by making a complaint against the accused. The court, as a public authority, must ensure that any interference with the right to privacy under article 8 is in accordance with the law, and is necessary in pursuit of a legitimate public interest...”

The court further held that there is no presumption that a complainant's mobile telephone or other devices should be inspected, retained or downloaded, any more than there is a presumption that investigators will attempt to look through material held in hard copy. There must be a properly identifiable foundation for the inquiry, not mere conjecture or speculation. Furthermore, as developed below, if there is a reasonable line of enquiry, the investigators should consider whether there are ways of readily accessing the information that do not involve looking at or taking possession of the complainant's mobile telephone or other digital device. If a reasonable line of inquiry is established to examine, for example, communications between a witness and a suspect, there may be a number of ways this can be achieved without the witness having to surrender their electronic device. The loss of such a device for any period of time may itself be an intrusion into their private life, even apart from considerations of privacy with respect to the contents. Thus the investigator will need to consider whether, depending on the apparent live issues, it may be possible to obtain all the relevant communications from the suspect's own

⁷² [2016] UKSC 26.

⁷³ [2020] EWCA CRIM 790.

mobile telephone or other devices without the need to inspect or download digital items held by the complainant.

The Human Rights Act, 1998 has rendered clarity on the existence of a right to privacy in UK jurisprudence and substantially resolved conflicting approaches regarding privacy in decided cases. The Human Rights Act, by incorporating the provisions of the European Convention on Human Rights (ECHR), has adopted the guarantee of the right to privacy into United Kingdom's domestic law. The Convention, together with its adoption into domestic legislation, has led to a considerable change in the development of protection of human privacy in English law. Also, the Data Protection Act, 1998 implemented in March, 2000, controls the compiling, and use of data relating to living individuals processed in the United Kingdom or elsewhere under the control of a United Kingdom established person or company, called a data controller. The Act limits the extent of data which may be stored, the processing of data and how it can be disclosed.

- Privacy in United States

In the USA, the protection of the right to privacy and the right to publicity is separate. Even though the latter is a subset of the former, it has been developed by judicial precedents in a unique manner, such that it is now a distinct right.

The evolution of the Privacy doctrine in the United States can be traced back in the case of *Boyd v. United States*⁷⁴ particularly shows that the Supreme Court, as early as 1885 recognized privacy as the underlying principle of the Fourth amendment prohibition against unlawful searches and seizures. Writing for the court, Justice Bradley recognized a concern for privacy as being part of heritage of British common law. Use of Fourth Amendment as a vehicle for the right of privacy was inhibited in the 1920s because of the heavy reliance placed on it by bootleggers during prohibition. Law is never created in a vacuum, and the interpretation of law, like the making of it, is shaped by the pressures and prejudices of the times. He held that:

“the principles laid down in this opinion affect the very essence of constitutional liberty and security. They apply to all invasions on the part of the government and its employees of the sanctity of a man's home and

⁷⁴ 116 US 616 (1886).

the privacies of life. It is not the breaking of his doors and the rummaging of his drawers that constitutes the essence of the offence, but it is the invasion of his indefeasible right of personal security, personal liberty, and private property, it is the invasion of this sacred right and any compulsory discovery by extorting the party's oath, or compelling the production of his private books and papers, to convict him of crime or to forfeit his property, is contrary to the principles of a free government... It may suit the purposes of despotic power, but it cannot abide the pure atmosphere of political liberty and personal freedom.”

Prior to 1967 when determining the reasonable expectation of privacy for purposes of discussing Fourth Amendment violations, the analysis was focused on whether the authority had trespassed on a private location. This trespass doctrine⁷⁵ was the prevailing test until *Katz*,⁷⁶ which extended the protection of the fourth amendment from ‘places’ to ‘people’, affording individuals more privacy even in public.

Justice Harlan in his judgment held that:

*“an enclosed telephone booth is an area where, like a home a person has a constitutionally protected reasonable expectation of privacy and that electronic, as well as physical, intrusion into a place that is in this sense private may constitute a violation of the Fourth Amendment.”*⁷⁷

The fourth amendment of the US constitution protects the individuals from unreasonable search and seizures from the government. It must be noted that it is an exception to the right against the search and seizures if it is done in reasonable sense.

The search under the fourth amendment includes the act of strip search where the private parts of a person can be searched. Electronic investigation is also a facet of search under the amendment and as a law it is infringement to the person’s right to privacy. Seizure under the fourth amendment means that the liberty of the individual is under the authority of the police officer who is arresting him and that person must submit his authority to the police officer. However, under the amendment the rule is

⁷⁵ *Olmstead v United States*, 277 US 438 (1928).

⁷⁶ 389 US 347 (1967).

⁷⁷ The Fourth Amendment (Amendment IV) to the United States Constitution prohibits unreasonable searches and seizures.

that the amendment protects the person's liberty against seizures and seizure is an exception under the law. In recent years, the fourth amendment's applicability in electronic searches and seizures has received much attention from the courts. With the advent of the internet and increased popularity of computers, there has been an increasing amount of crime occurring electronically. Consequently, evidence of such crime can often be found on computers, hard drives, or other electronic devices. The Fourth Amendment applies to the search and seizure of electronic devices.

Many electronic search cases involve whether law enforcement can search a company owned computer that an employee uses to conduct business. Although the case law is split, the majority holds that employees do not have a legitimate expectation of privacy with regard to information stored on a company owned computer. In the 2010 case of *City of Ontario v. Quon*,⁷⁸ the Supreme Court extended this lack of an expectation of privacy to text messages sent and received on an employer owned pager. The court had also observed that an individual does have a reasonable expectation of privacy provided that the seizure must meet with the test of reasonability.

*Griswold v. Connecticut*⁷⁹ gave its first and greatest recognition as a constitutional limitation on the power of both state and federal government to interfere in the lives of individuals. For the first time, the court found that the right of privacy to be sufficient importance to overturn a state law, that is, a Connecticut law prohibiting sale or distribution of contraceptives to any person.

In one of the most controversial cases, the Supreme Court found unconstitutional a Texas abortion statute which, like laws in force in most states, forbade procuring or attempting an abortion except by medical advice for the purpose of saving the life of the mother. In *Roe v. Wade*,⁸⁰ Justice Blackmun said that the state regulation violated the due process clause of the fourteenth amendment which was found to protect the right of privacy against state action. The right of privacy was said to be the basis of a woman's qualified right to procure an abortion free from state interference during most of her pregnancy.

⁷⁸ 560 US 746 (2010).

⁷⁹ Supra at note 14.

⁸⁰ 410 US 112 (1973).

On data protection, the United States felt some concerns about unauthorized use of personal information, and the invasions of privacy represented by personal data files finally achieved a level of redress in the Fair Credit Reporting Act, 1970.

Until the Act was passed, the average citizen had no recourse against the agencies that compiled and disseminated information that may have been used against them. There are various provisions in the Act that seek to protect privacy to some degree. Data Protection law ensures protection of living individuals with respect to the disclosure of personal data relating to them which is stored on computer. The United States of America has passed its Freedom of Information Act in 1966, enacted a Privacy Act in 1974 in order secure individual from embarrassing situations. The Privacy Act of 1974 is based on the congressional finding that:

- a. *“The maintenance of personal information systems by federal agencies directly affects the individual privacy.*
- b. *The proliferation of information systems, including computers, while necessary for the efficient and effective operation of the government presents a major potential for harm to individual privacy.*
- c. *It is necessary and proper for the Congress to control personal information systems operated by federal agencies in order to protect the privacy of individuals identified in their systems.”*

The Act rests on the principle that:

- i. There must be no personal data record keeping systems whose very existence is secret.
- ii. There must be a way for an individual to find out what information about him is in a record and how it is used.
- iii. There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
- iv. There must be a way for an individual to correct or amend a record of identifiable information about him, and any organization creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of

the data for their intended use and must take reasonable precautions to prevent misuse.⁸¹

- Privacy in European Union

In Europe, there is the European Convention on Human Rights (ECHR), 1953, an international agreement to protect human rights and fundamental freedoms in Europe. The second is the Charter of Fundamental Rights of the European Union (CFREU), 2000, a treaty enshrining certain political, social, and economic rights for the European Union. Under ECHR, the European Court of Human Rights (ECtHR), also known as the Strasbourg Court, is the adjudicating body, which hears complaints by individuals on alleged breaches of human rights by signatory states. Similarly, under CFREU, the Court of Justice of the European Union (CJEU), also called the Luxembourg Court, is the chief judicial authority of the European Union and oversees the uniform application and interpretation of European Union law, in co-operation with the national judiciary of the member states. However, India is not a signatory to any of the Charters.

Article 8 of the ECHR provides the right to respect for private and family life:

“1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”

Like in India, we have the reasonable restrictions under article 19(2) of the Indian Constitution, even in the article 8(2) we have some restrictions which can be made by the public authorities. The freedom of expression is considered as a subjective right

⁸¹ Hugh V. O'Neill, The Privacy Act of 1974: Introduction and Overview, American Educational Research Association, (1976).

under the article 8 when it comes to protection of rights such as the right to reputation and honor of a person, then the freedom of expression can be legitimately restricted.

Under the Charter, Article 7 respect for private and family life everyone has the right to respect for his or her private and family life, home and communications. Article 8 guarantees the protection of personal data. It mentions that everyone has the right to the protection of personal data concerning him or her and such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Clause 3 of the article says that compliance with these rules shall be subject to control by an independent authority.

Article 52 of the Charter mentions about the scope of guaranteed rights, these cover the limitation on the exercise of the rights and freedoms recognized by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interests recognized by the Union of the need to protect the rights and freedoms of others. Clause 2 protects the rights recognized by this Charter which are based on the Community Treaties or the Treaty on European Union shall be exercised under the conditions and within the limits defined by those Treaties.

Third clause of the same article provides that this Charter contains rights which correspond to rights guaranteed by the Convention of the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.

Article 52(3) provides for the ECHR as a minimum standard of human rights in the European Union. Article 52(3) thus leads the European Union to be indirectly bound by the ECHR as it must always be obeyed when restricting fundamental rights in the European Union. In order to understand the protection extended to the right to privacy in Union, the jurisprudence of Article 8 of the Convention and Article 7 of the Charter need to be analyzed. The term 'private life' is an essential ingredient of both these provisions and has been interpreted to encompass a wide range of interests.

Other than these Charters, the European Union enacted the General Data Protection Rules (GDPR), 2018 replacing the Data Protection Directive of 1995, which are said to be the strongest of the data protection rules till date. The GDPR applies to whole of the EU. This regulation contains provisions relating to the data of the individual, who can access the information of the individual, consent of the individuals and supervisory authority over the data of the individuals etc.

Article 4 of GDPR is a definition clause and defines ‘Personal Data’ in article 4(1) of GDPR⁸² and the term ‘processing’ in article 4(2) of the GDPR.⁸³ Under the article 4(1) of GDPR, personal data also includes the online identifiers (device identifiers, cookies, IP address tracker etc.) and location data of the individual as personal data. The definitions are very clear compared to the Personal Data Protection Bill, 2019 of India. In the GDPR, it is mandatory for the companies to seek consent before they collect or use a person’s data which is given under article 7 of the GDPR.⁸⁴ Chapter III of the GDPR provides for the rights of the data subject i.e. the individual from whom data is being taken. Under this there are several rights of the data subject such as providing information regarding the access to information, the right of access by the data subject, the right to rectify the information, right to erasure or right to be forgotten, right to restrict the processing of data or notifying the erasure of data, right to object etc., under article 34 of GDPR, any kind of data breach should be immediately reported to the authority under the GDPR and also to the individuals.

⁸² General Data Protection Regulation, 2018, Article 4(1): ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

⁸³ General Data Protection Regulation, 2018, Article 4(2): ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

⁸⁴ General Data Protection Regulation, 2018, Article 7: 1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data. 2. If the data subject’s consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding. 3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. 4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

In the case of *Niemietz v Germany*,⁸⁵ the ECtHR observed that the Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of private life. However, it would be too restrictive to limit the notion to an inner circle in which the individual may live his own personal life as he chooses and to exclude from entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings.

Similarly, in *Costello-Roberts v United Kingdom*,⁸⁶ the ECtHR stated that the notion of private life is a broad one and it is not susceptible to exhaustive definition. This broad approach is also present in the recent cases of European jurisprudence. In *S and Marper v United Kingdom*,⁸⁷ the ECtHR held, with respect to right to respect for private life, that:

“...the concept of ‘private life’... covers the physical and psychological integrity of a person... It can therefore embrace multiple aspects of the person's physical and social identity... Elements such as, for example, gender identification, name and sexual orientation and sexual life fall within the personal sphere protected by Article 8... Beyond a person's name, his or her private and family life may include other means of personal identification and of linking to a family... Information about the person's health is an important element of private life... The Court furthermore considers that an individual's ethnic identity must be regarded as another such element... The concept of private life moreover includes elements relating to a person's right to their image...”

In *Uzun v Germany*,⁸⁸ the European Court of Human Rights while examining an application claiming violation of Article 8 observed that:

“Article 8 protects, inter alia, a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world. There is, therefore, a zone of

⁸⁵ Application no. 13710/88, judgment dated 16th September 1992.

⁸⁶ Application no. 13134/87, judgment dated 25 March 1993.

⁸⁷ [2008] ECHR 1581.

⁸⁸ Application No. 35623/05 judgment dated 2nd September 2010.

interaction of a person with others, even in a public context, which may fall within the scope of “private life”...

There are a number of elements relevant to a consideration of whether a person's private life is concerned by measures affected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor...”

Thus, the determination of a complaint by an individual under Article 8 of the Convention necessarily involves a two stage test,⁸⁹ which can be summarized as below:

Stage 1: Article 8 Paragraph 1:

Does the complaint fall within the scope of one of the rights protected by Article 8 Para 1? If so, is there a positive obligation on the State to respect an individual's right and has it been fulfilled?

Stage 2: Article 8 Paragraph 2:

Has there been an interference with the Article 8 right? If so, is it in accordance with law? Does it pursue a legitimate aim? Is it necessary in a democratic society?

This test is followed by the Court each time it applies Article 8 in a given case. In other words, a fair balance is struck between the general interests of the community and the interests of the individual.

The Grand Chamber of 18 judges at the ECtHR, in *S and Marper v United Kingdom*,⁹⁰ examined the claim of the applicants that their Right to Respect for Private Life under Article 8 was being violated as their fingerprints, cell samples and DNA profiles were retained in a database after successful termination of criminal proceedings against them. The Court held that there had been a violation of Article 8

⁸⁹ Ursula Kilkelly, The right to respect for private and family life: A guide to the implementation of Article 8 of the European Convention on Human Rights, Council of Europe, (2001).

⁹⁰ Supra note 87.

of the Convention. Finding that the retention at issue had constituted a disproportionate interference with the applicants' right to respect for private life, the Court held that:

“the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons...fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation.”

It was further held that the mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8. However, in determining whether the personal information retained by the authorities involves any of the private life aspects mentioned above, the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained. Applying these principles, it was held that:

The Court notes at the outset that all three categories of the personal information retained by the authorities in the present cases, namely fingerprints, DNA profiles and cellular samples, constitute personal data within the meaning of the Data Protection Convention as they relate to identified or identifiable individuals. The Government accepted that all three categories are personal data within the meaning of the Data Protection Act 1998 in the hands of those who are able to identify the individual. Regarding the retention of cellular samples and DNA profiles, it was held that:

“Given the nature and the amount of personal information contained in cellular samples, their retention per se must be regarded as interfering with the right to respect for the private lives of the individuals concerned. That only a limited part of this information is actually extracted or used by the authorities through DNA profiling and that no immediate detriment is caused in a particular case does not change this conclusion... [T]he DNA profiles' capacity to provide a means of identifying genetic relationships between individuals... is in itself sufficient to conclude that their retention interferes with the right to the private life of the individuals concerned... The possibility the DNA profiles create for inferences to be drawn as to

ethnic origin makes their retention all the more sensitive and susceptible of affecting the right to private life.”

Regarding retention of fingerprints, it was held that:

“...fingerprints objectively contain unique information about the individual concerned allowing his or her identification with precision in a wide range of circumstances. They are thus capable of affecting his or her private life and retention of this information without the consent of the individual concerned cannot be regarded as neutral or insignificant...”

In *Uzun v Germany*,⁹¹ the ECtHR examined an application claiming violation of Article 8 of European Convention of Human Rights where the applicant’s data was obtained via the Global Positioning System (GPS) by the investigation agencies and was used against him in a criminal proceeding. In this case, the applicant was suspected of involvement in bomb attacks by the left-wing extremist movement. The Court unanimously concluded that there had been no violation of Article 8 and held that GPS surveillance of Mr. Uzun had been ordered to investigate several counts of attempted murder for which a terrorist movement had claimed responsibility and to prevent further bomb attacks. It therefore served the interests of national security and public safety, the prevention of crime and the protection of the rights of the victims. It had only been ordered after less intrusive methods of investigation had proved insufficient, for a relatively short period of time which was three months and it had affected Mr. Uzun only when he was travelling with his accomplice’s car. Therefore, he could not be said to have been subjected to total and comprehensive surveillance. Given that the investigation concerned very serious crimes, the Court found that the GPS surveillance of Mr. Uzun had been proportionate.

In *RE v The United Kingdom*,⁹² the applicant was arrested and detained on three occasions in relation to the murder of a police officer. He claimed violation of Article 8 under the regime of covert surveillance of consultations between detainees and their lawyers, medical advisors and appropriate adults sanctioned by the existing law. The ECtHR held that:

⁹¹ Supra note 88.

⁹² [2015] ECHR 947.

“The Court...considers that the surveillance of a legal consultation constitutes an extremely high degree of intrusion into a person’s right to respect for his or her private life and correspondence... Consequently, in such cases it will expect the same safeguards to be in place to protect individuals from arbitrary interference with their Article 8 rights. Surveillance of “appropriate adult”-detainee consultations were not subject to legal privilege and therefore a detainee would not have the same expectation of privacy....The relevant domestic provisions, insofar as they related to the possible surveillance of consultations between detainees and “appropriate adults”, were accompanied by “adequate safeguards against abuse”, notably as concerned the authorization, review and record keeping. Hence, there is no violation of Article 8.”

In *Roman Zakharov v Russia*,⁹³ ECtHR examined an application claiming violation of Article 8 of the Convention alleging that the mobile operators had permitted unrestricted interception of all telephone communications by the security services without prior judicial authorization, under the prevailing national law. The Court observed that:

“Mr. Zakharov was entitled to claim to be a victim of a violation of the European Convention even though he was unable to allege that he had been the subject of a concrete measure of surveillance. Given the secret nature of the surveillance measures provided for by the legislation, their broad scope (affecting all users of mobile telephone communications) and the lack of effective means to challenge them at national level... Russian law did not meet the quality of law requirement and was incapable of keeping the interception of communications to what was necessary in a democratic society. There had accordingly been a violation of Article 8 of the Convention.”

The European Courts have kept a balanced approach between individual interests and societal interests. The two step test in examining an individual claim related to a Convention right has strictly been followed by ECtHR.

⁹³ Application No. 47143/06, Judgment date 4 December 2015.

- International Instruments

The right to privacy is one of the human rights recognized in article 12 of the United Nations Declaration of Human Rights (UDHR), 1948 article 17 of the International Covenant on Civil and Political Rights (ICCPR), 1976 and in many other international and in many other international and regional treaties. The right to privacy was thus taken into the constitutional arena as an inherent right by many of the countries including the United States and India through judicial interpretations as well as constitutional amendments. The right to privacy was thus taken into the constitutional arena as an inherent right by many of the countries including the United States and India through judicial interpretations as well as constitutional amendments.

Article 12 of the Universal Declaration of Human Rights states

“No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, or to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks”⁹⁴

Article 17 of the International Covenant on Civil and Political Rights states—

“1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence and nor to unlawful attacks on his honor and reputation.

2. Everyone has the right to the protection of the law against such interference or attacks.”⁹⁵

The General Comment No. 16 to the article 17 of the International Covenant on Civil and Political Rights to which India is also a signatory emphasized on the need for laws relating to personal data mentions that the gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and

⁹⁴ Supra note 3.

⁹⁵ Supra note 4.

use it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for What purposes. Every individual should also be able to, ascertain which public authorizes or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.⁹⁶

The protection of privacy has been cherished as an essential human right. With the increasing technological advancements especially in the field of information and communications, the right to privacy and the protection of this right is heavily challenged. As a result, there arose many laws for data protection in many countries which focused on the protection of personal data of individuals. Nevertheless, it is difficult for the legislations to cope with the speed of the increasing technology and amend the laws on a continuous basis. The European Union (before the exit of UK) stated through their Charter of Fundamental Rights of the European Union⁹⁷ that everyone has the right to the protection of personal data concerning him or her. This statement is to be respected in terms of the protection of the personal data of individuals but to what extent this is put into practice.

One of the cases of visual privacy is of a leading actor Edison Chen from Hong Kong. His private sexual images were leaked into the internet in January 2008 where he was portrayed with women from the film industry.⁹⁸ For a period of time, this surfaced as the hot searches in China and the national as well as international police attempted to stop the spreading of the pictures but all their attempts were futile. They arrested a computer technician who repaired the laptop of that actor and stolen the pictures from them before posting on internet. Nevertheless, even after catching the culprit it is very difficult to control the widespread distribution of these pictures.

⁹⁶ UN HUMAN RIGHTS COMMITTEE, The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, CCPR General Comment No. 16: Article 17, HRI/GEN/1/Rev.9 (Vol. I).

⁹⁷ Charter of Fundamental Rights of the European Union, Article 8, pp. 10.

⁹⁸ Chang and Stewart, Sex, Rice, and Videotape: Popular Media, Transnational Asian/American Masculinity, and a Crisis of Privacy Law in the Edison Chen Sex Scandal, 37 *Amerasia Journal*, pp. 28, (2011).

- Other Countries

The decision in *Artavia Murillo ET AL. (“In Vitro Fertilization”) v Costa Rica*⁹⁹ (2012), addressed the question of whether the State’s prohibition on the practice of in vitro fertilization constituted an arbitrary interference with the right to private life. The Court held that:

“The scope of the protection of the right to private life has been interpreted in broad terms by the international human rights courts, when indicating that this goes beyond the right to privacy. The protection of private life encompasses a series of factors associated with the dignity of the individual, including, for example, the ability to develop his or her own personality and aspirations, to determine his or her own identity and to define his or her own personal relationships. The concept of private life encompasses aspects of physical and social identity, including the right to personal autonomy, personal development and the right to establish and develop relationships with other human beings and with the outside world. The effective exercise of the right to private life is decisive for the possibility of exercising personal autonomy on the future course of relevant events for a person’s quality of life. Private life includes the way in which individual views himself and how he decides to project this view towards others, and is an essential condition for the free development of the personality... Furthermore, the Court has indicated that motherhood is an essential part of the free development of a woman’s personality. Based on the foregoing, the Court considers that the decision of whether or not to become a parent is part of the right to private life and includes, in this case, the decision of whether or not to become a mother or father in the genetic or biological sense.”

In *Escher et al v Brazil*¹⁰⁰, telephonic interception and monitoring of telephonic lines was carried out by the military police of the State between April and June 1999. The Court found that the State violated the American Convention on Human Rights and held that Article 11 applies to telephone conversations irrespective of their content

⁹⁹ Inter-Am. Ct. H.R. (Ser. C) No. 257.

¹⁰⁰ Inter-Am. Ct. H.R. (Ser. C) No. 200.

and can even include both the technical operations designed to record this content by taping it and listening to it, or any other element of the communication process; for example, the destination or origin of the calls that are made, the identity of the speakers, the frequency, time and duration of the calls, aspects that can be verified without the need to record the content of the call by taping the conversation. Article 11 of the Convention recognizes that every person has the right to respect for his honor, prohibits an illegal attack against honor and reputation, and imposes on the States the obligation to provide legal protection against such attacks. In general, the right to honor relates to self-esteem and self-worth, while reputation refers to the opinion that others have of a person.

Owing to the inherent danger of abuse in any monitoring system, this measure must be based on especially precise legislation with clear, detailed rules. The American Convention protects the confidentiality and inviolability of communications from any kind of arbitrary or abusive interference from the State or individuals, consequently, the surveillance, intervention, recording and dissemination of such communications is prohibited, except in the cases established by law that are adapted to the objects and purposes of the American Convention.

In Canada, the Canadian Charter of Rights and Freedoms of 1982 does not explicitly provide for a right to privacy, certain sections of the Charter have been relied on by the Supreme Court of Canada to recognize a right to privacy. Privacy issues have been dealt in Section 7 and Section 8 of the Charter. In 1983, the Privacy Act was enacted to regulate how federal government collects, uses and discloses personal information.

In *Lavigne v. Canada (Office of the Commissioner of Official Languages)*,¹⁰¹ the Supreme Court of Canada recognized the Privacy Act as having a quasi-constitutional status, as it is closely linked to the values and rights set out in the Constitution. The Court also stated that the Privacy Act is a reminder of the extent to which the protection of privacy is necessary to the preservation of a free and democratic society.

The Personal Information Protection and Electronic Documents Act (PIPEDA), 2007 governs how private sector organizations collect, use and disclose personal

¹⁰¹ [2002] 2 SCR 773.

information in the course of commercial activities. One of the landmark cases on the right to privacy was *Hunter v Southam Inc.*¹⁰² this was also the first Supreme Court of Canada decision to consider Section 8 of the Charter. In this case, it was argued that Investigation Act had authorized several civil servants to enter the offices of Southam Inc and examine documents. The company claimed that this Act violated Section 8 of the Canadian Charter. The Court unanimously held that the Combines Investigation Act violated the Charter as it did not provide an appropriate standard for administering warrants.

Dickson J. wrote the opinion of the Court and observed that the Canadian Charter is a ‘purposive document’ whose purpose is to guarantee and to protect, within the limits of reason, the enjoyment of the rights and freedoms it enshrines and to constrain governmental action inconsistent with those rights and freedoms. The Court held that since Section 8 is an entrenched constitutional provision, it was not vulnerable to encroachment by legislative enactments in the same way as common law protections.

The Court held that the purpose of Section 8 is to protect an individual's reasonable expectation of privacy but right to privacy must be balanced against the government’s duty to enforce the law. It was further held that:

“The guarantee of security from unreasonable search and seizure only protects a reasonable expectation. This limitation on the right guaranteed by section 8, whether it is expressed negatively as freedom from unreasonable search and seizure, or positively as an entitlement to a “reasonable” expectation of privacy, indicates that an assessment must be made as to whether in a particular situation the public's interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance its goals, notably those of law enforcement.”

The decision in *R v Spencer*¹⁰³ was related to informational privacy. In this case, the appellant used online software to download child pornography onto a computer and shared it publicly. The police requested subscriber information associated with an IP address from the appellant’s Internet Service Provider and on the basis of it, searched

¹⁰² [1984] 2 SCR 145.

¹⁰³ 2014 SCC 43.

the computer used by him. The Canadian Supreme Court unanimously ruled that the request for an IP address infringed the Charter's guarantee against unreasonable search and seizure. It was held that the appellant had a reasonable expectation of privacy. In doing so, it assessed whether there is a reasonable expectation of privacy in the totality of the circumstances, which includes the nature of the privacy interests implicated by the state action and "factors more directly concerned with the expectation of privacy, both subjectively and objectively viewed, in relation to those interests". It was further held:

"...factors that may be considered in assessing the reasonable expectation of privacy can be grouped under four main headings for analytical convenience:

- a. the subject matter of the alleged search;*
- b. the claimant's interest in the subject matter;*
- c. the claimant's subjective expectation of privacy in the subject matter; and*
- d. whether this subjective expectation of privacy was objectively reasonable, having regard to the totality of the circumstances."*

The issue in the case was whether there is a privacy interest in subscriber information with respect to computers used in homes for private purposes. The Court applied a broad approach in understanding the online privacy interests and held that:

"Privacy is admittedly a "broad and somewhat evanescent concept"... [T]he Court has described three broad types of privacy interests - territorial, personal, and informational - which, while often overlapping, have proved helpful in identifying the nature of the privacy interest or interests at stake in particular situations..."

The Court found that the nature of appellant's privacy interest in subscriber information relating to a computer used privately was primarily an informational one and stated that the identity of a person linked to their use of the Internet must be recognized as giving rise to a privacy interest beyond that inherent in the person's name, address and telephone number found in the subscriber information.

It then set out three key elements of informational privacy, privacy as secrecy, privacy as control, and privacy as anonymity. It further emphasized on the importance of

anonymity in informational privacy, particularly in the age of the Internet and held that the anonymity may, depending on the totality of the circumstances, be the foundation of a privacy interest that engages constitutional protection against unreasonable search and seizure.

Though the Court stopped short of recognizing an absolute right to anonymity, it held that the anonymous Internet activity engages a high level of informational privacy. The Court further held that the disclosure of this information will often amount to the identification of a user with intimate or sensitive activities being carried out online, usually on the understanding that these activities would be anonymous. A request by a police officer that an ISP voluntarily disclose such information amounts to a search.

The Canadian Supreme Court has used provisions of the Charter to expand the scope of the right to privacy, used traditionally to protect individuals from an invasion of their property rights, to an individual's 'reasonable expectation of privacy'. The right to privacy has been held to be more than just a physical right as it includes the privacy in information about one's identity. Informational privacy has frequently been addressed under Section 8 of the Charter. Canadian privacy jurisprudence has developed with the advent of technology and the internet. Judicial decisions have significant implications for internet/digital privacy.

In South Africa, the right to privacy has been enshrined in Section 14 of the Bill of Rights in the 1996 Constitution. Section 14 provides that:

“14. Privacy - Everyone has the right to privacy, which includes the right not to have-

- a) Their person or home searched;*
- b) Their property searched;*
- c) Their possessions seized; or*
- d) The privacy of their communications infringed.”*

In *NM and Others v Smith and Others*,¹⁰⁴ the names of three women who were HIV positive were disclosed in a biography. They alleged that the publication, without their prior consent, violated their rights to privacy, dignity and psychological

¹⁰⁴ 2007 (5) SA 250 (CC).

integrity. The Court by majority held that the respondents were aware that the applicants had not given their express consent but had published their names, thereby violating their privacy and dignity rights.

Justice Madala delivered the majority judgment on the basis of the value of privacy and confidentiality in medical information and held that:

“Private and confidential medical information contains highly sensitive and personal information about individuals. The personal and intimate nature of an individual’s health information, unlike other forms of documentation, reflects delicate decisions and choices relating to issues pertaining to bodily and psychological integrity and personal autonomy. Individuals value the privacy of confidential medical information because of the vast number of people who could have access to the information and the potential harmful effects that may result from disclosure. The lack of respect for private medical information and its subsequent disclosure may result in fear jeopardizing an individual’s right to make certain fundamental choices that he/she has a right to make. There is therefore a strong privacy interest in maintaining confidentiality.”

The decision of the Court was that there must be a pressing social need for the right to privacy to be interfered with and that there was no such compelling public interest in this case. On the inter-relationship between the right to privacy, liberty and dignity, the Court observed that the right to privacy recognizes the importance of protecting the sphere of our personal daily lives from the public. In so doing, it highlights the inter-relationship between privacy, liberty and dignity as the key constitutional rights which construct our understanding of what it means to be a human being. All these rights are therefore interdependent and mutually reinforcing.

The court also mentioned that one must value privacy for a reason at least that the constitutional conception of being a human being asserts and seeks to foster the possibility of human beings choosing how to live their lives within the overall framework of a broader community.

CHAPTER V

DIGITAL PRIVACY IN MODERN WORLD

- Communication Privacy

Most nations around the globe control the attempt of interchanges by governments and private people and associations. These controls ordinarily appear to ensuring the security of interchanges and laws and guidelines that actualize those prerequisites.

There has been extraordinary responsibility on nations to embrace wiretapping laws to address new innovations. These laws are likewise in light of law implementation and knowledge offices strain to build reconnaissance capacities. In Japan, wiretapping was just endorsed as a legitimate technique for examination in 1999. Different nations, for example, Australia, Belgium, Germany, New Zealand, South Africa and the United Kingdom have all refreshed their laws to encourage reconnaissance of new innovations.

It is perceived worldwide that wiretapping and electronic surveillance are an exceptional types of examination that should just be utilized in restricted and bizarre conditions. Almost all significant peaceful accords on human rights shield the privilege of people from inappropriate intrusive observation.

Almost every country has sanctioned laws on the collection of phone, fax and message correspondences. In most of the nations, collection of data is started by law implementation agencies simply after it has been endorsed by an appointed authority or some other executive officer or significant level authority and by and large just for legal wrongdoings. Every now and again, it must be demonstrated that different sorts of examination were endeavoured and were not effective. There is some dissimilarity on what comprises an extreme offence.

A few nations including France and the United Kingdom have made legal commissions that audit wiretap utilization and look for privacy violations. These bodies have built up an aptitude in the zone that most adjudicators who approve reconnaissance, while they likewise can direct examinations once cases are finished. In different nations, the privacy official or information collection authority has some

capacity to lead oversight of electronic observation. Encryption and anonymous speech online are central to our right to privacy and to freedom of expression and of opinion. These rights are also enshrined in international human rights law¹⁰⁵ and are recognized as deserving of strong protections through encryption protocols.¹⁰⁶

Communities which have the threat of gross violations are especially influenced by access and accessibility of encrypted innovations. This is particularly evident in locales where the standard of law is not strict and the human privileges of explicit socioeconomics and minority communities are undermined. Unknown correspondences managed by encryption innovations give points of interest to communities who are oppressed by giving them safe gatherings to assemble, sort out, activate, and fabricate network. Right now, these encrypted protections will in general be enduring a problem in specific states which endeavour to either end access or catch encryption conventions.¹⁰⁷

A further test is the absence of encryption and privacy rights for the media and their sources. In spite of acknowledgment that opportunity of media is a foundation of democratic society, governments and intelligence offices have endeavoured to infringe upon this right. An absence of regard for mysterious correspondences rights helps government legitimization for getting to the substance and interchanges.

Private elements are progressively advancing on the web anonymity by executing encryption conventions and creating encoded correspondences applications. While this makes a serious market advantage as individuals search out best strategies for private interchanges, this segment is additionally confronting difficulties from different states. Intel organisations specifically are endeavouring to drive private associations to either give devices to encryption or open indirect accesses in explicit conditions, or to hand over encryption keys, now and again through simple errors of how encryption really functions. These encrypted applications are additionally either blocked or in danger of being obstructed in specific nations.

¹⁰⁵ Article 17 and Article 19 of UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations.

¹⁰⁶ UN HUMAN RIGHTS COUNCIL, Report of the Special Rapporteur on the Promotion and protection of the Right to Freedom of Opinion and Expression: Report to the Human Rights Council, David Kaye A/HRC/29/32.

¹⁰⁷ Jessica Conditt, Encrypted Chat App Signal Circumvents Government Censorship, Engadget, (21 December 2016).

States establishments and authorities, instead of endeavouring to shorten encryption, could set a main model by comprehension, underwriting, and receiving solid encryption conventions themselves. While the rights to protection and to freedom of expression are not supreme, they should be thoroughly shielded. The defensive estimates applied to private disconnected interchanges which work without the internet should likewise be embraced in on the web and computerized spaces. Encryption is in this manner a perfect technological way to deal with securing personal correspondences. Security by structure and default ought to be a focal component for growing new advancements. The Cambridge Analytica fiasco shows how harming innovations can be to security when the plan is focused just around for benefit or ease of use. Distinguishing potential security suggestions previously and during the improvement procedure is the most ideal path for new innovation to help ensure protection.

- Information Privacy

The overall case to protection of data incorporates such things as not to have our region attacked by outsiders, not to have our books perused, or our records played, or our garments worn, by others without our consent, regardless of whether this causes us no misfortune and educates those others nothing concerning us except for the zone of data security is smaller. Here, what we can guarantee is that others ought not to acquire information about us without our assent. In Professor Arthur Miller article¹⁰⁸ earlier, put it significantly more quickly characterizing it as the person's capacity to control the dissemination of data identifying with him.

This is the part of the overall right of security of data with which the current research is chiefly concerned, since it is the one which has been the most significantly influenced and some would state most hazardously undermined by ongoing advancements in data innovation. The misuse of such accumulated data by government agencies and private undertakings with or without express or certain assent from the information subjects is worth pondering. The exceptional reference of the use of the information by the private endeavours for the sake of web based business for topping off their coffers with salary got from such data.

The discussions on the right of security of data expanded during the 1960s and 1970s with the appearance of data innovation. The observation capability of amazing digital frameworks incited requests for explicit standards administering the storage and usage of individual data. The beginning of present day enactments around there can be followed to the principal information security law on the world ordered in the Land of Hesse in Germany in 1970. This was trailed by national laws in Sweden (1973), the United States (1974), Germany (1977) and France (1978).¹⁰⁹

Our era is an era of data. Data is information. Data is considered to have become new oil. The familiar saying that knowledge is power has obvious ramifications for the situation of the person where information is omnipresent, a widely inclusive. Innovation has made life in a general sense interconnected. The web has become

¹⁰⁸ Miller A.R, Assault on Privacy: Computers, Data Banks and Dossiers, University of Michigan Press, pp. 40, (1971).

¹⁰⁹ Directive 2006/24/EC of the European Parliament and the Council meeting of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

unavoidable as people invest increasingly more energy online every day of their lives. People interface with others and utilize the web as a method for correspondence. The web is utilized to carry on business and to purchase merchandise and ventures. People peruse the web looking for data, to send messages, utilize texting models and to download motion pictures. Online transactions have gotten a productive substitute for the day by day visit to the neighbouring store. Web based banking has redefined connections among investors and clients. Web based exchanging has made another stage for the market in protections. Online music has refashioned the radio. Online books have opened up another universe for the avid reader. The good old travel planner has been delivered repetitive by online interfaces which give everything from eateries to rest houses, aircraft passes to craftsmanship exhibitions, historical centre passes to music shows. These are a couple of the reasons individuals get to the web every day of their lives. However every exchange of an individual and each site that he or she visits leave electronic tracks for the most part without their insight. These electronic tracks contain amazing methods for data which give information on such an individual that the person is and their preferences. In fact, the data storehouses reveal the idea of the person, food choices, language preferences, wellbeing, side interests, sexual inclinations, kinships, methods of dress and political association. In accumulation, data gives an image of the being, of things which matter to him and those that don't, of things to be uncovered and those best covered up.¹¹⁰

Well known sites introduce cookie records by the client's program. Cookies can label programs for exceptional distinguished numbers, which permit them to perceive quick customers and secure data about online conduct. Data, particularly the perusing history of a person is used to make customer profiles. The utilization of calculations permits the formation of profiles about web using customers. Mechanized substance examination of messages takes into consideration perusing of their messages. An email can be broke down to find their interests and to target reasonable advertisements on the site of the window. The books which an individual buys online give impressions to focused publicizing of a similar classification. Regardless of whether an aircraft ticket has been bought on economy or business class, it gives fundamental data about work profile or spending limit of a person. Taxi rides set up

¹¹⁰ Francois Nawrot, Katarzyna Syska and Przemyslaw Switalski, Horizontal Application of Fundamental Rights - Right to Privacy on the Internet, 9th Annual European Constitutionalism Seminar, (May 2010).

for line to shopping centres give a profile of individual's inclinations. A lady who buys pregnancy related drugs online would be in line to get advertisements for child items. Lives are available for electronic investigation. To say the least, security concerns are truly an issue in the time of data.

The era of data driven society has brought about complex issues for enlightening privacy. These issues emerge from the idea of data itself. Data has three aspects: it is shared publicly, dissimilar and recombinant. There can be concurrent individuals of the usage of a snippet of data by one individual doesn't make it less accessible to another. Furthermore, attacks of information security are hard to recognize on the grounds that they can be dissimilar. Data can be gotten to, put away and dispersed without notice. Its capacity to go at the speed of light improves the imperceptibility of access to information and data collection can be the swiftest robbery of all. Thirdly, data is recombinant as in information can be utilized as a contribution to collect more information. Individually, these information silos may seem inconsequential. In aggregation, they disclose the nature of the personality: food habits, language, health, hobbies, sexual preferences, friendships, ways of dress and political affiliation. In aggregation, information provides a picture of the being: of things which matter and those that don't, of things to be disclosed and those best hidden.¹¹¹

- Individual Privacy

It is important to address one key fact that has made more significance by the improvement of both covert observation on gadgets and data preparing innovation. In the event that the decision of the individual is fundamental to individual security, both in the feeling of permitting physical interruptions and of sharing data, in what capacity would privacy be able to be supposed to be attacked by the getting of data about an individual and its handling via programmed implies if the individual has no information this is happening? A simple answer lies in the chilling impact convention initially enunciated by the US Supreme Court. As the West German Constitutional Court said in its 1983 decision holding another Census Act not according to constitutional principles that:

¹¹¹ Christina P. Moniodis, Moving from Nixon to NASA: Privacy's Second Strand - A Right to Informational Privacy, Yale Journal of Law and Technology, Vol. 15 (1), pp. 153, (2013).

“If someone cannot predict with sufficient certainty which information about himself in certain areas is known to his social milieu, and cannot estimate sufficiently the knowledge of parties to whom communication may possibly be made, he is crucially inhibited in his freedom to plan or decide freely and without being subject to any pressure or influence (i.e. self-determined). The right to self-determination in relation to information precludes a social order and a legal order enabling it, in which the citizens no longer can know who knows what, when and on what occasion about them. If someone is uncertain whether deviant behaviour is noted down and stored permanently as information, or is applied or passed on, he will try not to attract attention by such behaviour. If he reckons that participation in assembly or a citizen initiative will be registered officially and that personal risks might result from it, he may possibly renounce the exercise of his respective rights. This would not only impair his chances of development but would also impair the common good because self-determination is an elementary functional condition of a free democratic community based on its citizens’ capacity to act and to cooperate.”

These lines spotlight the restricting impact on the activity of different freedoms of realizing that one is, or might be, subject to limitation. It is only the state of similar dystopia that was also communicated in George Orwell’s 1984.

There might be threat in such a turn of events on the off chance that it is to the detriment of individual rights, since it is consistently hard to make statutory bodies that are adequately autonomous of those that are present. In any case, this progress is basic to shield people from ill-advised observation of which they might know, just as giving a viable answer for the topic of how to determine the troublesome cases in which reconnaissance might be legitimate without overcoming conceivable reasons by exposure to the individual concerned.

The ongoing pattern leading from the expansion in innovation and web utilization prompted the monitoring and surveillance of the information by the administrative agencies. Practically all the nations check and direct the information that is streaming to and from their nation as to check whether they are in accordance with the current laws of that state or not. The legislatures keep track through the network access

suppliers (ISP's) and the intermediaries, for example, social media platforms, who act as boundaries between the residents and the access to the web. The legislatures relying upon their need on specific conditions confine such access to the web. For example, in case of national emergency or security of the state etc the administrations welcome the ISP's to ensure that they don't have any sites which advance or show unfortunate substance. We can see the state of China where the ISP's are to screen the utilization of web by the residents and report any sort of misappropriation to their authorities.

Data mining forms along with information revelation can be joined to generate data about people. Metadata and the development like internet of things can rethink human presence in manners which are yet completely to be seen. This, as Christina Moniodis states in her lighting up article¹¹² brings about the formation of new information about people, something which even she or he didn't have, this stances major issue for the court. During a time of rapid advancing innovation it is outlandish for an adjudicator to think about all the potential utilization of data:

“...The creation of new knowledge complicates data privacy law as it involves information the individual did not possess and could not disclose, knowingly or otherwise. In addition, as our state becomes an “information state” through increasing reliance on information – such that information is described as the “lifeblood that sustains political, social, and business decisions. It becomes impossible to conceptualize all of the possible uses of information and resulting harms. Such a situation poses a challenge for courts who are effectively asked to anticipate and remedy invisible, evolving harms.” The contemporary age has been aptly regarded as “an era of ubiquitous data surveillance, or the systematic monitoring of citizen’s communications or actions through the use of information technology”

It is substantially a period of ‘big data’ or the gathering of huge informational index. This informational index is equipped for being looked, that it has linkages with other informational collections and is set apart by the comprehensive extension and the permanency of collection of information. The difficulties posed by big data postures

¹¹² Ibid.

to the security of data come from state and non-state elements. Individuals who use wearable gadgets and online mediums may not think about themselves as having chipped in information yet their exercises of utilization and commitment bring about the age of immense measures of information about individual ways of life, decisions and inclinations. Yvonne McDermott¹¹³ specifies about the invested self in these terms:

“...The rise in the so called quantified self, or the self-tracking of biological, environmental, physical, or behavioural information through tracking devices, Internet-of-things devices, social network data and other means may result in information being gathered not just about the individual user, but about people around them as well. Thus, a solely consent based model does not entirely ensure the protection of one’s data, especially when data collected for one purpose can be repurposed for another. Businesses and governments often aggregate a variety of information fragments, including pieces of information which may not be viewed as private in isolation to create a detailed portrait of personalities and behaviour of individuals.”

The harmony between information guidelines and individual privacy raises complex issues requiring sensitive amendments to be drawn between the authentic problem of the State on one hand and individual issues for the assurance of protection of data on the other. The need of protection of data extends toward one side to those personal issues to which a sensible desire for privacy may join. It communicates an option to be left alone. A more progressive study which has developed in scholastic writing of a relatively ongoing cause is identified with the assurance of one’s personality. Information security relates intimately with the present scenario. Information, for example, health data would be a classification to which a sensible effort for protection comes. There might be other kinds of information which falls outside the scope. Aside from protecting the data, information protection systems try to ensure the rights of the person. This is clear from the legislation in the European data protection system on the chief basis of assent.

¹¹³ Yvonne McDermott, Conceptualizing the Right to Data Protection in an Era of Big Data, Leiden Journal of International Law, pp. 244, (2017).

Concerning the issue of consent is the prerequisite of transparent government whose structure requires a revelation by the information beneficiary of data relating to information sharing and its usage. Another purview from which information protection frameworks can protect individuals, is that they must ensure the impartiality which guarantees that the collection of information ought to be completed in a way which is not based on racial or ethnic sources, political or religious convictions, hereditary or health status or sexual preferences.

Digital privacy violations can compromise monetary frameworks including banking system. Encryption can be the terrorist's closest companion, and his security of data has been upgraded by the equivalent standards as of normal individual, that have both made information mining doable and has inspired tremendous amounts of individual data from honest people. The web with its anonymity and the safe encryption of digitized information which, when joined with that anonymity can make the cyber world an integral asset of unlawful activities. The legislature also has a genuine need to introspect digitization with regards to national security.

The proliferation of biometrics and other data collection methods in everyday life for access to financial services, other daily need services, infrastructure, and mobile technology etc., can affect privacy of an individual due to the sensitivity of the data collected without proper procedure or legislative measure.¹¹⁴

- Individual Privacy and Security of State under Indian Laws

Section 5 of the Telegraph Act, 1885 mandates the Central Government and the State Government to arrange to block attempt of messages on two conditions:

1. *“In the occurrence of any ‘public emergency’ or in the interest of ‘public safety’, and*
2. *If it is considered necessary or expedient to do so, in addition to the following instances: in the interests of the sovereignty and integrity of India; the security of the State; friendly relations with foreign states; public order; and for the prevention of incitement to the commission of an offense.”*

¹¹⁴ Yue Liu, Privacy Regulations on Biometrics in Australia, Computer Law & Security Review, Vol. 2, pp. 6, (2010).

In 2007, Rule 419A was annexed to the Indian Telegraph Rules, (1951) under the Indian Telegraph Act. These Rules give that the permission to the interception of interchanges must be given by the Secretary in the Ministry of Home Affairs on account of the Central Government and the Secretary to the State Government responsible for the Home Department on account of a State Government. In any case, the Rules give that in unavoidable conditions a request can likewise be given by an official, not underneath the position of a Joint Secretary to the Government of India, who has been approved by the Union Home Secretary or the State Home Secretary.

The Unlawful Activities Prevention Act, 1967 takes into consideration that data gathered through interception of communication (under the Information Technology Act or the Telegraph Act) to be created as an evidence for an offense under the Act. Also, the intercepted communications are not acceptable except if the accused person is given a duplicate for the request endorsing the intercept attempt, in this way making unlawful interference unacceptable.

Section 26 of the Indian Post Office Act, 1898 enables the Central Government and the State Governments of India to check postal articles. Section 26 of the Act specifically expresses that:

“on the occurrence of any public emergency or in the interest of public safety or tranquillity, the Central Government, State Government or any officer specially authorised by the Central or State Government may direct the interception, detention or disposal of any postal article, class or description of postal articles in the course of transmission by post.” and

“If any doubt arises regarding the existence of public emergency, public safety or tranquillity then a certificate to that effect by the Central Government or a State Government would be considered conclusive proof of such a condition being satisfied.”

Section 91 of the Code of Criminal Procedure, 1973 regulates targeted access to stored content. In particular, section 91 states that

“A Court in India or any officer in charge of a police station may summon a person to produce any document or any other "thing" that is necessary

for the purposes of any investigation, inquiry, trial or other proceeding under the Code of Criminal Procedure.”

Under the same section, law enforcement bodies in India can get permission to access information. In any event that the Commissioner of Police or Superintendent of Police accepts that such information is required for the aforementioned purposes. He may require the postal administration to confine such document on a request from a court. Section 92 of the Code likewise permits District Magistrates and Courts to give directions requiring report or ‘other things’ inside the custody of any postal administration to be submitted before it if necessary with the end goal of any examination, inquiry, trial or other purposes under the Code. There are minimal legal clarifications regarding the matter however it has been contended that it is conceivable to encrypt the provisions under the code in a manner that even private Internet Service Providers can be considered as postal authorities and along these lines become private or public bodies with the scope of this code. The degree of protection required for postal bodies under section 92 is higher than that given to an ordinary person under section 91 since even a police personnel is accountable for a police headquarters and can request things to be delivered, though under section 92 it must be either the District Magistrate or a particular Court.

Under section 3 of the Indian Wireless Telegraphy Act, 1933, the custody of wireless telegraphy elements without valid permission or a license leads to unlawful act. Further, the unauthorised bodies or persons for maintenance or to carry function of wireless communications networks for the objectives of monitoring, intercepting communications and surveillance is infringement of the Wireless Telegraphy Act.

Aadhaar Act, 2016 in its section 33(1) does not allow sharing of data, including personal data or consent records, aside from when it is by a request for a court not substandard compared to that of a District Judge. The greater part conclusion read down this arrangements expressing that a person, whose data is tried to be delivered, will be managed a chance of hearing the option to challenge such a request passed by moving toward the higher court. The affected individual would likewise have the option to protest the revelation of data on acknowledged grounds in law, including Article 20(3) and Article 21 of the Constitution.

Section 47 of the Aadhaar Act famously accommodated the cognizance of offense under the Act just on a grievance made by the UIDAI or any official or individual approved by it. The larger part of assessment clarified that it should be amended to incorporate a clause where a person whose rights have been abused by under the Aadhaar Act can file a complaint to appropriate authority.

Section 57 allowed the utilization of the Aadhaar system for building up the personal data of a person 'for any reason'. This arrangement was perused down to imply that such a reason must be supported by law. Further, at whatever point any such 'law' is made, it is dependent upon the interpreting authorities.

Another kind of surveillance instrument named AarogyaSetu app was introduced by the government in the COVID-19 pandemic situation. The AarogyaSetu app is a contact tracing app developed by the National Informatics Centre under the Ministry of Electronics & Information Technology, which enables the people to know whether there exists a corona virus case in their close locality.

It achieves this using the phone's Bluetooth and GPS capabilities. The app will keep a record of all other AarogyaSetu users that it detected nearby using Bluetooth, and also a GPS log of all the places that the device had been at fifteen minute intervals. These records are stored on the phone till the time any user tests positive or declares symptoms of COVID-19 in a self assessment survey in the app. In such cases, the records are uploaded to the servers.

While registering, the app collects a set of personal information such as name, sex, age, phone number, current location and travel history that is uploaded to government servers, which then generates a unique digital identity for that user. When the Bluetooth of two AarogyaSetu users sniff each other out, this unique digital identity is exchanged along with the time and location of the meeting.

The privacy concerns with the app are firstly there is a privacy law vacuum that is India. With no legislation that spells out in detail how the online privacy of Indians is to be protected, AarogyaSetu users have little choice but to accept the privacy policy provided by the government. The policy goes into some detail on where and how long the data will be retained, but it leaves the language around who will have access to it vague. As per the policy, *'persons carrying out medical and administrative*

interventions necessary in relation to COVID-19 will have access to the data. Also, the details of the application's technical architecture and its source code have not been made public and the application is not backed by any legislation whatsoever. Nobody knows how much data the application will collect and how much data will be shared and used.

Data profiling is the using of the combined data to identify, categorise and segregate to make decisions about the individuals who are known to the decision maker through their computerised profile. Governments as well as companies use data profiling to build the profiles on individual persons. One of the examples of data profiling emerged after a woman sued the US based metro mail when one of their data entry clerks caught up her basing on the information she provided in a survey. Upon hearing the case it occurred that the metro mail maintained a twenty five page dossier about the woman which includes her information on the usage of her haemorrhoid medicine, her income details etc.¹¹⁵

In countries where there are privacy laws, the companies de-identify the data of the individuals though which can be used when they are cross referenced from the national census which consists of all the details of individuals collected through offline mode.

¹¹⁵ Electronic Privacy Information Center, [Privacy and Consumer Profiling](#), last accessed 26 June 2020.

CHAPTER VI

CONCLUSION AND SUGGESTIONS

Formulation of a regime for data protection is a complex exercise which needs to be undertaken by the State after a careful balancing of the requirements of privacy coupled with other values which the protection of data serves together with the legitimate concerns of the State. One of the chief concerns which the formulation of a data protection regime has to take into account is that while the internet is a source of lawful activity, both personal and commercial and concerns of national security conundrums since the seamless structure of the internet can be exploited by non-law abiding instruments to wreak havoc and destruction in civilised societies. As long as intelligence personnel can be trusted to use the knowledge gained only for the defense of the nation, the public will be compensated for the costs of diminished privacy in increased security from terrorist attacks¹¹⁶

Apart from national security, the state may have justifiable reasons for the collection and storage of data. In a social welfare state, the government embarks upon programs which provide benefits to impoverished and marginalized sections of society. There is a vital state interest in ensuring that scarce public resources are not dissipated by the diversion of resources to persons who do not qualify as recipients. Allocation of resources for human development is coupled with a legitimate concern that the utilization of resources should not be siphoned away for extraneous purposes. Data mining with the object of ensuring that resources are properly deployed to legitimate beneficiaries is a valid ground for the state to insist on the collection of authentic data. But, the data which the state has collected has to be utilized for legitimate purposes of the state and ought not to be utilized unauthorized for extraneous purposes. This will ensure that the legitimate concerns of the state are duly safeguarded while, at the same time, protecting privacy concerns. Prevention and investigation of crime and protection of the revenue are among the legitimate aims of the state. Digital platforms are a vital tool of ensuring good governance in a social welfare state. Information technology which is legitimately deployed is a powerful enabler in the spread of innovation and knowledge.

¹¹⁶ Ibid.

Privacy involves hiding information whereas anonymity involves hiding what makes it personal. An unauthorized parting of the medical records of an individual which have been furnished to a hospital will amount to an invasion of privacy. On the other hand, the state may assert a legitimate interest in analyzing data borne from hospital records to understand and deal with a public health epidemic such as malaria or dengue to obviate a serious impact on the population. If the State preserves the anonymity of the individual it could legitimately assert a valid state interest in the preservation of public health to design appropriate policy interventions on the basis of the data available to it.¹¹⁷

Pre-surveillance authorization from a judicial or quasi-judicial authority, which is not too proximate to the institutions carrying out the surveillance, and only where there is clear evidence of a sufficient threat and the surveillance proposed, is strictly necessary and proportionate. An effective and accessible remedy for people subjected to unlawful surveillance, including post notification and the possibility of civil compensation and criminal sanction for unlawful surveillance.

Indian legislations by a large way primarily concerned with the security of the state however in the digital era times have changed and since law is ever evolving it is the time to make necessary amendments into the contemporary law of the country which will serve greater protection to the data of individuals. The Indian Data Protection Bill, 2019 readily provides a system which will direct the parties and business organizations to be concerned about the personal data. The Bill provides a change in framework and organization in the businesses which also is beneficial for the ordinary person. However, the drawbacks of the draft legislation, which are mentioned in this study, must be appropriately addressed before it becomes a law.

¹¹⁷ Jeffrey M. Skopek, Reasonable Expectations of Anonymity, Virginia Law Review, Vol. 101, pp. 691, (2015).

BIBLIOGRAPHY

A. BOOKS

Cooley, Thomas, A TREATISE ON THE LAW OF TORTS, 2nd Edition, pp.29, (1888).

R. Shama Shastri, KAUTILA'S ARTHASASTRA, pp. 19 (1961).

Richard Hixson, PRIVACY IN A PUBLIC SOCIETY: HUMAN RIGHTS IN CONFLICT, Oxford University Press, pp. 255 (1987).

Barrington Moore, PRIVACY: STUDIES IN SOCIAL AND CULTURAL HISTORY, M.E. Sharpe, pp. 48, (1984).

Prosser, Keeton, ON LAW OF TORTS, West Group, (1987).

Lucas A. Power, THE FOURTH ESTATE AND THE CONSTITUTION, Berkeley: University of California Press (1991).

V.R. Krishna Iyer, ESSAYS ON PRESS FREEDOM, Capital Foundation Society, (1996).

D. S. Trivedi, SECRET SERVICE IN ANCIENT INDIA, Allied Publishers Pvt. Ltd. (1988).

Hyman Gross, PRIVACY - ITS LEGAL PROTECTION, Oceana Publications, (1976).

Richard F. Hixon, PRIVACY IN PUBLIC SOCIETY, Oxford University Press, pp. 183, (1987).

Denning, WHAT NEXT IN THE LAW?, OUP Oxford pp. 219, (1982).

Ursula Kilkelly, THE RIGHT TO RESPECT FOR PRIVATE AND FAMILY LIFE: A GUIDE TO THE IMPLEMENTATION OF ARTICLE 8 OF THE EUROPEAN CONVENTION ON HUMAN RIGHTS, Council of Europe, (2001).

Miller A.R, ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS AND DOSSIERS, University of Michigan Press, pp. 40, (1971).

B. JOURNALS

Edward Shils, *Privacy: Its Constitution and Vicissitudes*, *Law and Contemporary Problems*, pp. 281-306, (1966).

Rana P.K., *Right to Privacy in Indian Perspective*, *International Journal of Law*, pp. 7, (2016).

Anna Jonsson Cornell, *Right to Privacy*, *Max Planck Encyclopedia of Comparative Constitutional Law*, (2015).

Hugh V. O'Neill, *The Privacy Act of 1974: Introduction and Overview*, *American Educational Research Association*, (1976).

Chang and Stewart, *Sex, Rice, and Videotape: Popular Media, Transnational Asian/American Masculinity, and a Crisis of Privacy Law in the Edison Chen Sex Scandal*, *37 Amerasia Journal*, pp. 28, (2011).

Jessica Conditt, *Encrypted Chat App Signal Circumvents Government Censorship*, *Engadget*, (2016).

Francois Nawrot, Katarzyna Syska and Przemyslaw Switalski, *Horizontal Application of Fundamental Rights - Right to Privacy on the Internet*, *9th Annual European Constitutionalism Seminar*, (2010).

Christina P. Moniodis, *Moving from Nixon to NASA: Privacy's Second Strand - A Right to Informational Privacy*, *15 Yale J. of Law & Technology* (2013).

Yvonne McDermott, *Conceptualizing the Right to Data Protection in an Era of Big Data*, *Leiden Journal of International Law*, pp. 244, (2017).

Yue Liu, *Privacy Regulations on Biometrics in Australia*, *Computer Law & Security Review*, Vol. 2, pp. 6, (2010).

Jeffrey M. Skopek, *Reasonable Expectations of Anonymity*, *Virginia Law Review*, Vol. 101, pp. 691, (2015).

C. WEB SOURCES

Branagan, T., China boosts internet surveillance, THE GUARDIAN, <http://www.guardian.co.uk/world/2011/jul/26/china-boosts-internet-surveillance> (June 16, 2020)

Cavoukian, A., Whole body imaging in airport scanners: building in privacy by design, INFORMATION & PRIVACY COMMISSIONER, ONTARIO, CANADA. <http://www.ipc.on.ca/images/resources/wholebodyimaging.pdf> (June 8, 2020)

Internet matters: the net's sweeping impact on growth, jobs and prosperity, MCKINSEY GLOBAL INSTITUTE) http://www.eg8forum.com/fr/documents/actualities/McKinsey_and_company-internet_matters.pdf (June 11, 2020)

Klein, Jay, Digging Deeper into Data Packet Inspection, SECURITY AND PROTECTION OF INFORMATION, UNIVERITY OF DEFENCE IN BRNO, <http://spi.unob.cz/papers/2007/2007-06.pdf> (June 27, 2020)

Konvitz, Milton R., Privacy and the Law: A Philosophical Prelude, 31 Law and Contemp. Probs., no. 2 (Spring 1966), <https://scholarship.law.duke.edu/lcp/vol31/iss2/3> (May 5, 2020)

Massimino, E., Privacy, Free Expression and the facebook standard, FORBES, <http://forbes.com/sites/realspin/2012/01/31/privacy-free-expression-and-the-facebook-standard/> (May 18, 2020)

MILLER, FRED D., Aristotle's Political Theory, THE STANFORD ENCYCLOPEDIA OF PHILOSOPHY, <https://plato.stanford.edu/archives/win2017/entries/aristotle-politics/> (May 10, 2020)

Netter, W., The Death of Privacy, PRIVACY MODULE I: DATA PROFILING INTRODUCTION, UNIVERSITY OF HARVARD, http://cyber.law.harvard.edu/privacy/module2_intro.html (May 28, 2020)

Protalanski, E., Facebook has over 845 million users, ZDNET, <https://www.zdnet.com/blog/facebook/facebook-has-over-845-million-users/8332> (June 18, 2020)

Rotenburg M. & Hoofnagle C., Submission to the House Government Reform Committee on Data Mining, <http://epic.org/privacy/profiling/datamining3.25.03.html> (May 25, 2003)

Shils, Edward, Privacy: Its Constitution and Vicissitudes, 31 Law and Contemp. Probs., no.2 (Spring 1966) <https://scholarship.law.duke.edu/lcp/vol31/iss2/4> (July 5, 2020)

Sweeney, L. Strategies for De-identifying patient data for research, (1998) Carnegie Mellon University, Data Privacy Lab, http://www.ocri.ca/ehip/2005/presentations/sweeney_bw.pdf (June 28, 2020)