EXPLORING THE NEED OF LEGISLATION TO PROTECT THE RIGHT TO PRIVACY IN INDIA: A CRITICAL STUDY

Dissertation submitted to National Law University and Judicial Academy, Assam in partial fulfilment for award of the degree of

MASTER OF LAWS

Supervised by

Gitanjali Ghosh

(Assistant Professor of Law)

Submitted by

Shehnaz Aziz

UID: SF0217014

2017-18

National Law University and Judicial Academy, Assam

2 July, 2018

SUPERVISOR CERTIFICATE

It is to certify that Ms. Shehnaz Aziz is pursuing Master of Laws (LL.M.) from National Law University, Assam and has completed his dissertation titled "EXPLORING THE NEED OF LEGISLATION TO PROTECT THE RIGHT TO PRIVACY IN INDIA: A CRITICAL STUDY" under my supervision. The research work is found to be original and suitable for submission.

Gitanjali Ghosh

Date: 02.07.2018 **(Assistant Professor of Law)**

DECLARATION

I, Ms. Shehnaz Aziz, pursuing Master of Laws (LL.M.) from National Law University, Assam, do hereby declare that the present dissertation titled "EXPLORING THE NEED OF LEGISLATION TO PROTECT THE RIGHT TO PRIVACY IN INDIA: A CRITICAL STUDY" is an original research work and has not been submitted, either in part or full anywhere else for any purpose, academic or otherwise, to the best of my knowledge.

Date : 02.07.2018

Shehnaz Aziz

UID: SF0217014

ACKNOWLEDGEMENT

It brings me great pleasure for an opportunity to submit my dissertation titled "EXPLORING THE NEED OF LEGISLATION TO PROTECT THE RIGHT TO PRIVACY IN INDIA: A CRITICAL STUDY" as an integral part of my LLM programme. For this I am deeply indebted and sincerely thankful to Mrs. Gitanjali Ghosh, Assistant Professor of Law, National Law University, Assam, for her help, invaluable guidance and encouragement throughout the course of present work.

I am also thankful to Prof. (Dr.) J.S. Patil, Vice-Chancellor, National Law University, Assam for allotting the dissertation topic as per my area of research interest.

Finally, I am deeply thankful to my parents and teachers who helped and inspired me in completing this research.

Shehnaz Aziz

UID: SF0217014

PREFACE

Privacy has been defined in several ways over last hundreds of years. Judge *Thomas Cooley* called it as a right to be let alone. Time and again philosophers, scholars and Jurists tried to lament the difficulty to satisfy the concept of privacy. Aurther *Miller* in his work has declared

privacy as difficult to define as its nature is exasperatingly vague and evanescent. Privacy is a

sweeping concept, encompassing (among other things) freedom of thought, control over one's

body, solitude in one's home, control over information about oneself, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations. But it is also pertinent to understand that 'Privacy' is one of the most nebulous terms our society has ever chanced upon. In the recent years, there have been debates on Right to Privacy, its safeguards, reasonable restrictions against this right, various positions and non-recognition of this right by some courts, and the ongoing debate on the existence of a constitutional Right to Privacy. Many Indian jurists have raised the question that, "While there is a right to life, is there a right to privacy?" This raises a very difficult conundrum for constitutional jurists that while one has the right to life, does that also entail the right to enjoy a life of their own choice,

devoid of any public scrutiny. There is no clear understanding of the different paradigms of the right to privacy, and there exists a lack of a theoretical framework to help us in this respect. There is no second thought that privacy plays one of the most integral part of a man's life and is as important as the right to live. But since we know that India falls under the umbrella of those rare nations whose constitution has not given cognizance to Privacy rights in its queue of Fundamental Rights, hence the development of this new right is attracting so much attention both at national and international level.

Considering the aforementioned analysis, the first chapter of the dissertation explores the origin of the right to privacy and tries to give a comprehensive idea of what privacy right is about and the need to mark the term privacy as a right. The chapter also throws light on the objectives, research problem and hypotheses of the dissertation, foundations on which the entire research has been done.

The dissertation in its second chapter introduces the subject matter where it begins with the understanding and analyzing the philosophical and constitutional aspects behind the evolutionary principles of the term privacy and its development and stipulation in it gaining the status of a right . Also, the chapter has concentrated on the definational aspects of the same to study the basic anonymity which revolves around the defination of privacy and it as a right and how is differs among different cultures and individuals.

The third chapter of the dissertation examines the major themes that emerged with the researcher attempts to make a comparative outlook of the status of privacy rights in India to that of other nations of the world. The chapter also evaluates that the international instruments and the importance of privacy as a rights which later settles on the analysis that keeping in mind or looking into the progress and development of the international instruments and judicial trend, there should be a separate positive law enacted, giving status to the term privacy as a right and protection from the law.

The fourth chapter duly analyse the laws relating to right to privacy in India and the judicious role of the higher Indian judiciary to protect the privacy rights of an individual interpreting the very Constitution and the provisions of those laws which are related to the privacy rights of the people. Nevertheless, the chapter goes on to analyse the requirement with the swelling technological changes and in a techno-friendly era where the violation of privacy rights is more prominent, the need of an absolute positive law to protect the privacy rights of the people of India directly in any form of violation, without being waiting for the decision of the judiciary to come pursuing whether such a violation is even a violation of privacy rights or not.

The fifth chapter of the dissertation examines the privacy issues and the recent trends that have been most visible and contentious of late in order to speculate on the future of privacy jurisprudence. The chapter evaluates the strong modern media and technological advances which has a dire impact on the very existence of the privacy rights of an individual and hence the need to enact an absolute positive law for the protection of those rights directly in the court of law.

At the end, the dissertation in its sixth chapter makes the concluding remarks and suggestions evidencing and verifying the hypothesis of the research work. The dissertation also includes a chronology of pertinent and an annotated bibliography of useful works on privacy law.

TABLE OF CASES

TABLE OF STATUTES, CONVENTIONS, COMMISSIONS AND REPORTS

S.No.	*Statutes, Conventions, Reports and Commissions*
1.	African Charter on the Rights and Welfare of the Child- 1990.
2.	African Union Principles on Freedom of Expression (the right of access to information)- 2002.
3.	American Convention on Human Rights- 1969.
4.	American Declaration of the Rights and Duties of Man- 1948.
5.	Arab Charter on Human Rights- 1994.
6.	ASEAN Human Rights Declaration- 2012.
7.	Constitution of India- 1950
8.	European Convention on Human Rights- 1950.
9.	India Post Office Act- 1898.
10.	Indian Evidence Act- 1872.
11.	Information Technology Act- 2000.
12.	Information Technology Act- 2008.
13.	International Covenant on Civil and Political Rights- 1976.
14.	Justice ManepalliNarayanaRaoVenkatachalliah Commission- 2000.
15.	Medical Termination of Pregnancy Act- 1971.
16.	Right to Information Act- 2005.
17.	The Code of Criminal Procedure- 1973.
18.	The Indian Telegraph Act- 1885.
19.	UN Convention on the Rights of the Child- 1989.
20.	United Nations Convention on Migrant Workers- 1994.
21.	Universal Declaration of Human Rights- 1948.

TABLE OF ABBREVIATIONS

1.	Anr.	Another
2.	Art.	Article
3.	Cl.	Clause
4.	Corpn.	Corporation
5.	Del	Delhi
6.	DPSP	Directive Principle of State Policies
7.	Ed.	Edition
8.	*et al.*	and others
9.	HC	High Court
10.	Hon'ble	Honourable
11.	*Id*	Ibidem
12.	J.	Justice
13.	Ltd.	Limited
14.	Mad.	Madras
15.	No.	Number
16.	Op. cit	Opere citato
17.	Ors.	Others
18.	p.	Page Number
19.	S.	Section
20.	SC	Supreme Court
21.	*Supra note*	Above
22.	UOI	Union of India
23.	v.	Versus
24.	Vol.	Volume

TABLE OF CONTENT

CHAPTER 1

INTRODUCTION

'Privacy' is a notoriously difficult concept to define and cannot be understood as a static andone-dimensional concept. It can only be construed as a group of rights.[1] The general idea of privacy can be conceptualized as the practices or acts which we want to protect from public scrutiny.[2] The principle of privacy rights was first referred to as a human right and elaborated in the pioneering article of *Warren and Brandies,* titled "The right to privacy"[3]. Numerous philosophers have indirectly referred to the concept of privacy in their work. A classic example would be *Aristotle's* identification of two spheres of an individual's life namely the 'polis' or the public sphere, and 'oikos' or the private sphere.[4]*Jeremy Bentham* had also recognised the existence of a "private" element in an individual's life[5]. Even *Shakespeare* had his own notions of private, which he said was the 'undeclared' and included a sense of social secrecy[6].

However, a concern that the opposition to the right to privacy immediately raises, is how do we define 'privacy' and the scope of application of a right to privacy? A good approach through which privacy can be defined is to strike a balance between the reductionist and the antireductionist attempts at defining privacy.[7] The reductionist philosophy would state that the ambit of privacy and its violation should be specified by the legislature.[8] The advantage of this approach would be that it would allow the legislature to operationalize privacy and thus include privacy as a fundamental right. However, it would end up limiting the scope of privacy and the extent to which judicial review can improve it.

---

1 J. L. MILLS, THE LOST RIGHT 4 (Oxford University Press 2008).

2 JA CANNATACI, THE INDIVIDUAL AND PRIVACY (Routledge 2015).

3 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 205, 193-220 (1890).

4 ARISTOTLE, B. JOWETT AND H.W.C. DAVIS, ARISTOTLE'S POLITICS (Clarendon Press 1908).

5 Glenn Negley, *Philosophical Views on the value of Privacy*, 31 LAW & CONTEMP. PROBS. 321-22 (1966).

6 HUEBERT, RONALD, PRIVACY IN THE AGE OF SHAKESPEARE (University of Toronto Press 2015).

7 UjwalaUppaluri&VarshaShivanagowda, *Preserving Constitutive Values in the Modern Panopticon: The Case for Legislating toward a Privacy Right in India*, 5 NUJS L. REV. 21 (2012).

8 Madison Powers, *A Cognitive Access Definition of Privacy*, 15 LAW & PHILO. 369 (1996).

On the other hand, the anti-reductionist philosophy would take a broader approach through which a wider range of interferences with persons and personal spaces are viewed as raising.[9] An advantage of this approach would be that it will widen the ambit of the right. However, it would end up in leaving vague interpretations of privacy. Therefore, it is the view that a balance should be struck between these two approaches. The Indian legislature should provide a wide scope of the various kinds of privacy and its violations. Further, they should provide a definition of privacy with a specific Act being enacted which allows the judiciary to encompass any changes and further review the right to privacy.

1.1.Research Problem

Every institution is liable to be abused,and every liberty, if left unbridled, has the tendency to become a lisence which would lead to disorder and anarchy. This is the threshold on which we are standing today. Televesion channels in a bid to increase their TRP ratings are resorting to sensationalized journalism with a view to earn a competitive edge over the others. The press is overstepping in every direction the obvious bound of propriety and of decency. Gossip is no longer the resource of the ideal and the vicious but has become the trade which is pursued with industry as well as effrontery. The newspaper is looked upon as a saleble commodity like any other, and design and sensational titles, obscenity and vulgarity dominate the rest.

Sting operations have now became the order of the day. They are a part of the hectic pace at which the media is evolving, carrying with every sting as much promise as risk. However, though technology cannot be thwarted but it has its limits. It cannot be denied that it is of practical importance that a precarious balance between the fundamental right to expression and the right to ones privacy be maintained. The second practice which has become more of a daily occurrence now is that of Media Trials. Something which started to show to the public at large the truth about cases, which now has became a practice interfering dangerously with the justice delivery system.

Todays's advancement in technology gives the modern media powerful new tools for intrusion into private lives. Cameras are smaller and easier to hide.

9 *Id.*

Conversations are easily recorded surreptitiously. Computers and the internet provide the ability to rummage through the closets of your life in ways that have never before been possible. The carrying out of an sting operation may be an expressionof the right to free press but it caries with it an indomitable duty to respect the privacy of others. The individual who is the subject of the press or televesion 'item' has his or her personality, reputation or career dashed to ground after the media exposure. He too has a fundamental right to live with dignity and respect and a right to privacy guaranteed to him under the inclusiove meaning of Article 21 of the Indian Constitution.

Today, it is being witnessed that the over-inquisitive media, which is a product of over- commercialization, is severely encroaching the individual's right to privacy by crossing the boundaries of its freedom. Recently, it has assumed dangerous proportions, to the extent of intruding into very privacy of individuals. Gross misuse of technological advancements and the unhealthy competition in the field of journalism resulted in obliteration of norms or commitment to the noble profession.Government at all levels have the capacity to gather and retain huge amounts of information about their citizens including personal information saying from health, education and vital statistics to details about businesses, insurance, and banking activities. And whenever and wherever vast amount of private information are held, there is always someone who wants the information and someone else also will use it in destructive ways.

Analysis of what is being done to penetrate individual privacy through current surveillance technology and the prospects for technological advance in the next decate, as well as the counter-measures now available, may conveniently be divided into three categories. These are physical surveillance, the observation without his knowledge or consent of a person's location, acts, speech, or private records through listening or watching devices; data surveillance, the collection, storage, exchange and integration of comprehensive documentary information about individuals and groups through computers and other data-processing system; and psychological surveillance, the use of mental testings, drugs, emotion-measuring devices, and other processes to extract information which the individual does not know he is revealing, reveals unwillingly, or discloses without full awareness of the exposure of his private personality.Basically, the government collects the personal information of its citizens for the security of the state, to prevent tax evasion or for any other public good. And people trust the government

that their personal information will be protected. But there are many instances where the government has breached the trust of Indian Citizens as it failed to protect the personal data collected for public purpose, some of which will be broadly discussed in the later part of the dissertation paper.

Currently, the all-seeing eye need not necessarily belong to the government, as many in the private sector find it valuable to conduct various forms of surveillance or to "mine" data collected by others. So these private enterprises are selling the collected data to advertisers and other companies. Social network websites like Facebook and Twitter had not even energed and companies were just beginning to recognise the databases that they could use for marketing. All the people voluntarily disclose their personal information on these sites. People put their own snaps or private details on the web through blogs and social networking sites. With the fast developing technological advancements the current law is insufficient, where due to non existence of any specific law or defination with regard to that of the concept of privacy, it emanated as a foremost research problem is the topic of dissertation.In short, there is no clear understanding of the different paradigms of the right to privacy, and there exists a lack of a theoretical framework to help us in this respect.

Privacy is essential for the development of inner and outer contents of all human beings. Having measures for the protection of psychological privacy by every legal system will be beneficial for the society at large. The present research problem rest on the idea that because being unchecked, the repercussions of the overreaching powers of a techno-friendly society and privacy-destroying technologies is leading us to the naked society, where privacy is zero and where this right has rarely survive. Gradually, it has also affected the mental and psychological privacy of every human being which is being considered as the basic edifice of the civilization. For that matter, a comprehensive socio-legal study is required in order to strengthen the present legal control mechanism and update the law with advancement of technology by making the privacy right an absolute positive right in India.

1.2.Aim

'Privacy' is one of the most nebulous terms our society has ever chanced upon. In the recent years, there have been debates on Right to Privacy, its safeguards, reasonable restrictions against this right, various positions and non-recognition of this right by some Courts, and the ongoing debate on the existence of a constitutional Right to Privacy. Many Indian jurists have raised the question that, "While there is a right to life, is there a right to privacy?" This raises a very difficult conundrum for constitutional jurists that while one has the right to life, does that also entail the right to enjoy a life of their own choice, devoid of any public scrutiny. The aim of this paper is to understand and study the term privacy and the existence of it being as a right, to examine the challenges it is facing within the era of technological advancementsand modern media and the need of an enacted law /statute defining and giving validity to the term privacy which is directly enforceable in the Court of law.

1.3.Objectives

- To study the philosophical and definitional aspects of right to privacy.
- To analyse the international instruments and comparative outlook of right to privacy in relation with India and other states.
- To examine the laws relating to right to privacy in India and the role of higher judiciary in validating the term.
- To understand the vicissitudes in the concept of right to privacy and its standing in recent trends with the existence of a techno-friendly era.

1.4.Scope and Limitations

The scope of the research relies upon the exploration and scrutinization of the term privacy and probing the significance of converting it into a right with the help of analyzing the comparative outlook of right to privacy in India with other nations, study of international instruments, examination of relating laws and recent trends of right to privacy along with the judicial interpretation of the same. The research also tried to

understand the modern advancement of technology and media, and the need of an hour to make a concrete absolute positive legislation in the country of India for the better protection and promotion of the privacy rights for the individuals.Hence considering the aforementioned purpose, the research in the present dissertation has delimited its studiesof the comparative outlook of nations to mainly two countries, namely USA and UK. Further, the research was also limited in studying only certain heads of right to privacy in Indiai.e. the right to privacy and communications, privacy and home, privacy of bodily integrity and right to privacy of records, where the dissertation has restricted itself from studying other heads of privacy rights as that of financial privacy, genetic privacy and others, for the absolute reason of paucity of time and limited resouces.

1.5.Detailed Review of Literature

Richard A. Glenn, in his book "THE RIGHT TO PRIVACY: RIGHTS AND LIBERTIES UNDER THE LAW"(ABC-CLIO, Inc., 2003), illuminates the controversial nature of constitutional right to privacy in US. He explores the origins of the right to privacy in United States examining the philosophical, constitutional and common law foundations, trogh the ideas of various thinkers and philosophers. In his book the author tries to undertand and examine the need of converting privacy as a right and the importance of giving it a constitutional status for the protection and promotion of the rights of the individuals. The author further moves ahead with the contentious issues which are preventing the term privacy to gain its validity as a positive right which is justified by the very Constitution of the United States of America. Along with this the author also made an elaborate study of the role of higher judiciary in protectiong and nurturing the privacy rights as a fundamental right of one's existence. The given literature has stronglyhelped in the research work of the present dissertation, to make a comparative outlook of the existing status of the right to privacy in US to that of India and the need to provide the privacy right the standing of a positive absolute right in both the countries. Though the literature lacked in tracing the importance and status of privacy rights in other countries apart from that of US, still it has helped immensely in making a comparative analysis of US and Indian laws for the purpose of this dissertation.

Justice Yatindra Singh, in his book "CYBER LAWS" (Universal Law Publishing, 6th ed. 2016), under chapter XIII explores the idea and importance of the data protection laws in India under the head of cyber law, for the protection and promotion of one's privacy rights from getting violated. The author in this chapter has extensively studied about the raising danger of modern media and advancement in technologies making today's era a techno-friendly era, which forces the need in current trend for the formulation of privacy/data protection laws, to protect the public and private information's of an individual from getting intruded. The literature has greatly substantiated in understanding the need of a positive absolute law for the protection of one's privacy rights in need of the research work of present dissertation.

Aashit Shah and Nilesh Zacharias, in their article "DATA PRIVACY AND DATA PROTECTION", Nishith Desai Associates(2001), studies the international instruments along-side the Indian legal scenario (judicial intervention), to understand the term privacy, need for the recognition of term privacy as a fundamental right and the necessity of protection of those privacy rights by the respective government by enacting an absolute positive law in their respective countries. The article also provides with the necessary policies and steps a government should follow while drafting the legislation to protect the privacy rights of its citizens, which in return has assisted in a great extent in the present research work to understand the international instruments validating the privacy rights and the need of it to be reflected in a concrete law form.

Utkarsh Amar, in his article "RIGHT TO PRIVACY IN THE DAWN OF INFORMATION AND COMMUNICATION TECHNOLOGY- A CRITICAL REVIEW, 3 International Journal of Law and Legal Jurisprudence Studies (2012), tries to evaluate the present role of modern media and the advancement in technologies, on the right to privacy of the Indian people.The authors states that different governmental schemes which empower the government to delve into all the information of its citizens have raised serious questions on the existence of privacy rights of the citizens. India being an emerging economy is seen as a viable market at the global level but such viability stands vulnerable if Indian law is not in conformity with its business counterparts. Privacy plays one of the most integral part of a man's life and is as important as the right to live. But since we know that India falls under the umbrella of those rare nations whose constitution has not given cognizance to Privacy rights in its

queue of Fundamental Rights, hence the development of this new right is attracting so much attention both at national and international level. Hence, the understanding of privacy rights, the role of media and technological advancements and the government requirement to take initiatives in the form of an absolute law to protect the privacy rights of its citizens, has helped enormously in the present research work to prove/disprove the hypotheses of the dissertation.

SatyaVratYadav and Vasundhara Anil Kaul, in their article "RIGHT TO PRIVACY: REDEFINING SOCIAL SECURITY IN INDIA"3 International Journal of Law and Legal Jurisprudence Studies (2012), explores the debate of the Indian polity on merits and demerits of clouding data of one and all citizens of the country through UID system ever since the concept of AADHAAR has been introduced. As stated in the article, the UID system carry necessary biometric data, which if falls in the wrong hands can be very dangerous to the society. It's one of the few possible consequences may be identity theft. Hence, the research of both the authors in the present research paper revolves around the idea of the technological advancements and its impact on the government schemes like Aadhaar, which has a great possibility of the violation of privacy rights of any individual. Hence therefore, the current literature has helped the present research work of the dissertation in understanding the recent trends in India along-side the involvement of the technological advances and modern media in a techno-friendly era.

SuhrithParthasarathy, in his article "PRIVACY, AADHAAR AND CONSTITUTION"The Hindu Centre for Politics and Public Policy (2017), studies the various international instruments acknowledging the privacy rights and the judicial trend in India validating those instruments and norms, interpreting implicitly right to privacy within the fundamental meaning of Art. 21 of the Constitution of India. The current literature has helped to understand various laws which are related to privacy rights in India and how judiciary has given an upper hand to the concepts of public interest and national security over the individual's right to privacy. This has further helped in the present research work of dissertation in understanding the point that privacy right cannot be solely left with judiciary for its interpretation and validation and hence requires a positive absolute law/legislation for its protection in the Court of law.

Samuel D. Warren & Louis D. Brandeis, in their paper “THE RIGHT TO PRIVACY” 4 HARV. L. REV. (1890), for the first time coined the idea of privacy rights which was referred to as a human right in their work. The authors tried to understand the term privacy and the necessity of making it or converting it into a right for the overall fundamental growth of an individual. The current literature has assisted in the second chapterof the dissertation to understand the philosophical and definitional aspects of right to privacy and to explore how fundamental it is for the normal existence of a human being.

1.6.Hypotheses

The present hypothesis rests on the presumption that if unchecked, the repercussions of the overreaching powers of a techno-friendly society and privacy-destroying technologies shall lead us to the naked society, where privacy will be zero and where this right will rarely survive.

The second hypothesis largely rests on the conjecture that, the right to privacy as a right is not protected to a great magnitude in the country of India as there exist no concrete absolute positive law to support its existence.

1.7.Research Questions

- What is privacy in the eyes of law?
- How has the concept of right to privacy evolved in the law?
- What is the impact of a techno-friendly era/society on the concept of privacy rights in India?
- What is the need of making privacy right an absolute positive right in India?

1.8.Research Methodology

Research Method

The present research work has required the theoretical study where it has dealt with the literature relating to value and importance of privacy attached to different cultures or societies, media and technologies intrusion in individual privacy, protection

of right to privacy by Constitution, legislative measures or some other governmental policies, and international conventions and treaties with respect to the protection of individual privacy. Hence, the methodology employed for the dissertation is limited primarily on the doctrinal research as it is concerned with legal prepositions and doctrine. Since the methods of the research are confined to the study of books and the pertinent internet sources, the research for the project did not acquire field work to look into the status of the Right to Privacy in India and hence are not opinion oriented which otherwise would have made adoption of non-doctrinal research the more conducive choice for the study where a wider view of varying perspectives could be examined through surveys and other forms of such data collection lending to it, the necessary detail to the study rendering it a comprehensive study. Another reason for adoption of the doctrinal research method was the fact that it is the study of law and not that of society which is needed for the project at hand and which can be efficiently accomplished through research in library. Doctrinal research also promotes objectivity which is a necessary requirement, given the clinicality of the subject.

Research Design and Sources of Data Collection

The research design which was opted in the dissertation is that of the exploratory, explanatory and descriptive research design. The former was opted to make an initial research into a hypothetical or theoretical idea of the concepts like that of privacy, privacy as a right and others. The second design mainly helped to look into the cause and effect relationship between the concept of privacy and the essence of it as a right and other different factors affecting such rights in India as such and lastly, the descriptive design was used in order to make an attempt to explore and explain while providing additional information about a topic. The sources of data collection are both primary and secondary sources of data collection, where the primary sources mainly consists of the cases, judgments, statutes, commission reports, executive rules, etc. and the secondary sources comprising that of the books, articles, journals, web sources and others cradles respectively.

CHAPTER 2

PHILOSOPHICAL AND DEFINITIONAL ASPECTS OF RIGHT TO PRIVACY: AN ANALYSIS

Privacy has been defined and demarcated in several ways over hundread of years in different countries drawing from its social pattern and values of a specific societal, political and economic compass. The contentious part in outlining the term helds with the question of studying the term in general or giving privacy the status of a human right, those minimal rights which individuals need to have against the state of other public authority by virtue of their being members of the human family, irrespective of any other consideration[10].

2.1.Meaning and Definition of Privacy

In general, the term privacy has been derived from Latin word: privatus meaning thereby 'separated from the rest, deprived of something, esp. office, participation in the government', in turn privatus has been derived from term privo 'to deprive'. Privacy is the ability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves selectively. The boundaries and content of what is considered private differ among cultures and individuals, but share basic common themes. Privacy is sometimes related to anonymity, the wish to remain unnoticed or unidentified in the public realm. When something is private to a person, it usually means there is something within them that is considered inherently special or personally sensitive[11].

Hence, the concept of privacy rests on the promise that 'a certain private sphere of individual liberty will be kept largely beyond the reach of Government' and it embodies the acceptance of the 'moral fact that a person belongs to himself and not to others nor to society as a whole'.[12] Gerety defines privacy as an autonomy or control

---

10 LohitD.Naikar, *The Law Relating to Human Rights*, BANGALORE PULANI AND PULANI 3 (2004).

11 ArchanaParashar, *Right to have Rights: Supreme Court as the Guarantor of Rights of Persons with Mental/ Intellectual Disability*, 5 THE INDIAN JOURNAL OF CONSTITUTIONAL LAW 160 (2011).

12 Thornburgh v. American College of Obstetricians &Gynecologists, 476 US 747, 772 (1986).

over the intimacies of personal identity[13]. He identifies three broad concepts in the legal definition of privacy-intimacy, identity and autonomy.[14]*Bostwick* relies upon a threefold classification of privacy: the privacy of repose, the privacy of sanctuary and the privacy of intimate decision[15].

Solove adopts a pragmatic approach and identifies necessary and sufficient conditions for the right to privacy. He divides privacy into six comprehensive (though not mutually exclusive) rights: (i) the right to be let alone; (ii) limited access to the self-the ability to shield oneself from others; (iii) secrecy-concealing certain matters from others; (iv) control over personal information; (v) personhood-the protection of one's personality, individuality and dignity; and (vi) intimacy-control over or limiting access to intimate relationships.[16]

The question here comes till what extent the government can or is the government of a particular state given with the authority to curtail ones right to privacy in any particular instance?If the Government interferes with my right to speak to an audience in an open maidan, can it be said that my right to privacy has been infringed? The answer is in the negative. In such cases, my right to the freedom of speech is interfered with. However, if the Government interferes with my right to speak to my brother in the confines of my home, can I say that my right to privacy has been intruded upon? The answer must necessarily be in the affirmative.[17] The right to privacy thus emphasizes upon the place in which the act occurs. It was this principle that prompted *Douglas, J.* to enunciate the repulsive notion of invading marital bedrooms for telltale signs of crime.[18]

However, the question can be formulated and asked again if one go to bazar or for that matter any public space and there one has a conversation with his father, and in that instance the government comes in the picture and averts oneself from doing so, is then the right to privacy of that person is infringed, in spite of the fact that the communication/ conversation was made in an open public area? The answer once more

13 R. Revathi, *Pervasive Technology, Invasive Privacy and Lucrative Piracy*, 51 JILI 368 (2009).
14 *Id.*
15 Jed Rubenfield, *The Right to Privacy*, 102 HARV. L. REV. 737, 740 (1989).
16 Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087-1088 (2002).
17 Griswold v. Connecticut, 381 US 479, 485 (1965).
18 *Id.*

is in the affirmative. It thus appears that the right to privacy is hinged not only upon the place, but more specifically, upon an arena which by its very nature is secluded from access to the public. The nature of the act or the communication must be such as is inherently personal and private. Extending privacy protection to the spheres of marriage, procreation, contraception, family relationships, child-rearing and education is thus justified[19].

An attempt at defining privacy is of no use if the levels of abstraction do not translate into concrete specifics[20]. Broadly speaking, privacy law deals with freedom of thought, control over one's body, peace and solitude in one's home, control of information regarding oneself, freedom from surveillance,[21] protection from unreasonable search and seizure and protection of reputation[22], which in all form has to be protected and promoted by the governmental and non-governmental set-up of the state respectively.

2.2. Privacy as a Right and its Efficacy

In 1859, *John Stuart* in his essay 'On Liberty' gave expression to the need to preserve a zone within which the liberty of the citizen would be free from the authority of the state, where later it took its first concrete form in the 1890s, when *Samuel Warren and Louis Brandeis* developed the concept of privacy; they identified the 'injury to the feelings' and recognized it as a legal injury and through invasions upon his privacy, subjected him to mental pain and distress. Their philosophy is spiritual rather than mundane or material. To set up the philosophy 'right to privacy' they first

19 Solove, *supra note 16.*

20 *Id.*

21 The early Indian privacy cases dealt exclusively with police surveillance of habitual criminals. See e.g. Kharak Singh v. State of U.P AIR 1295(SC 1963) (challenging Chapter XX of the U.P. Police Regulations which placed possible criminals under surveillance); Gobind v. State of M.P 2 SCC 148 (1975) (challenging the validity of Regulations 855 and 856 of the M.P. Police Regulations, which permitted the police to keep an uncomfortable surveillance on individuals suspected of perpetrating crime).

22 The Fourth Amendment of the US Constitution provides a safeguard from unreasonable search and seizure, and no search can be carried out without a warrant issued on probable cause. The Supreme Court has not allowed Fourth Amendment developments to percolate into the Indian Constitution. See M.P. Sharma v. Satish Chandra AIR 300 (SC 1954) (rejecting the premise that search and seizure violates the principle of self-incrimination embedded in Article 20(3) of the Constitution). But see District Registrar and Collector v. Canara Bank 1 SCC 496 (2005) (finding the Andhra Pradesh Amendment to Section 73 of the Stamp Act, 1899, to be unconstitutional since it permitted search and seizure on private premises). See infra I.B.2. Search and Seizure: The Fourth Amendment.

try to establish it as a part of right to life, and then they compare it with tort of defamation (damage to reputation), implied contract of not disclose. Finally they come to conclusion that object of privacy is to protect 'inviolate personality'; and not mere to related to private property[23].

It is further noted that there also exist an all together different view point on the idea of whether thr tem privacy to be studied in general or should be given the status of a right which can be further ascertained by the law. Some experts assert that in fact the right to privacy should not be defined as a separate legal right at all. By their reasoning, existing laws relating to privacy in general should be sufficient.[24] Other experts, such as *Dean Prosser*, have attempted, but failed, to find a "common ground" between the leading kinds of privacy cases in the Court system, at least to formulate a definition.[25]However, one law school treatise from Israel, however, on the subject of 'privacy in the digital environment', suggests that the 'right to privacy should be seen as an independent right that deserves legal protection in itself.' It has therefore proposed a working definition for a 'right to privacy':

> *The right to privacy is our right to keep a domain around us, which includes all those things that are part of us, such as our body, home, thoughts, feelings, secrets and identity. The right to privacy gives us the ability to choose which parts in this domain can be accessed by others, and to control the extent, manner and timing of the use of those parts we choose to disclose*[26].

Social patterns and values today are too diverse, decentralised, and purposefully different to provide a foundation for general rules of discourse at the level of specificity required for the protection of privacy. This does not imply that a legal concept of privacy should be disregarded; instead, protection can be defined as specifically or as generally as the legislature chooses by taking into consideration the cultural context and allow its contours to fit within the social and also

---

23 Warren, *supra* note 3, at 193.

24 *Privacy in the Digital Environment*, HAIFA CENTRE OF LAW & TECHNOLOGY 1-12 (2005).

25 Tom Gerety, *Redefining Privacy*, 12 HARV. C.R.C. L. L. REV. 233, 241 (1977).

26 *Id.*

economic conditions. It is important that we explore these foundations for the purposes of identifying the assumptions, assessing its justifications, and analysing the paradoxical effects of India's privacy policies.[27]

The idea of privacy is intimately connected with the conception of liberty, justice, human dignity, individuality and family life. Although the concept of privacy is a longstanding phenomenon, codification of privacy as a right is rather new. Further, as societies go through a fundamental transformation, it also creates the need for re-conceptualising the right to privacy. The question arises in terms of how far it should be protected and against what? Most scholars tend to define privacy within the confines of their specific research. For example, privacy as the 'right to be let alone' is a rather simple concept and cannot be used in a meaningful way. Such a narrowly constructed conception of privacy in obvious ways is restricted in its utility[28]. *Gavison* argues that, "not letting people alone' cannot readily be described as an invasion of privacy".[29]But it can also be argued that what counts as a right to privacy, then, has the potential of having important consequences on a variety of scales. Hence, inevitably, the demands of the modern society and technological changes require a redefinition of the right to privacy[30].

Again, during the existence of the former controversies and contentions, another question pops up as that of does everybody in society is liable to acquire equal and similardefense in relation to that of privacy and how far privacy is indispensablefor the existence of one human being? Every individual should have the same claim to privacy. Thus, one individual's exercise of privacy must submit to the equal claim of every other individual to the same exercise. However, in reality, this does entail some loss of privacy for everybody[31]. *Gavison* argues that there is a loss of privacy when others obtain information about an individual, pay attention to him or her, or gain access to him or her. It is suggested that the concept of privacy consists of a complex combination of three elements that is secrecy, anonymity and solitude.[32]While these

---

27 A. Manoj Krishna, *Privacy Revisited*, 24 THE ACADEMY LAW REVIEW 52, 41-75 (2000).

28 RAYMOND WACKS, PERSONAL INFORMATION: PRIVACY AND THE LAW 15-18 (Clarendon Press 2003) (1993).

29 Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 437 (1980).

30 *Id.*

31 *Id.*

32 *Id*. at 428.

elements are independent of each other, they are also related. Privacy therefore consists of the individual's control over access to, and information about, himself or herself.[33]An individual who chooses to disclose certain aspects of his or her private life cannot experience a loss of privacy on the ground that others gain access to him or her. On the contrary, if the individual chooses not to allow others to gain access to himself or herself, or his or her personal information, then any intrusion into his or her private affairs or a disclosure of his or her personal information would violate his or her right of privacy. Therefore, the variation in the quality of privacy is dependent on the extent and frequency with which an individual is 'exposed' to the public. It seems reasonable to suppose that, as with other social values, some inequality in the distribution of privacy does exist.[34]

It is with this purpose that distinction is required in 'informational privacy' from 'decisional privacy.' The focus of decisional privacy is on freedom from interference when making certain fundamental decisions. In contrast, informational privacy is concerned with the use, transfer, and processing of personal data generated in daily life. The extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others' attention.[35]This approach has been criticised on the ground that if a loss of privacy occurs whenever any information about an individual becomes known, then the concept of privacy loses its intuitive meaning. Such a proposition leads to the awkward result that any loss of the solitude of, or information about, an individual becomes a loss of privacy.[36]

In contrary to approaches like *Gavison's, Wacks* argues that a limiting or controlling factor is required. He points out that although focusing attention upon an individual or intruding upon his solitude is inherently objectionable in its own right, our concern for the individual's privacy in these circumstances is strongest when the person is engaging in activities that we would normally consider private. He suggests that the protection afforded by the law of privacy should be limited to information 'which

---

33 James Rachels, *Why Privacy is Important?* 4 PHIL. & PUB. AFF. 326, 323-340 (1975).

34 COLIN J. BENNETT & CHARLES D. RAAB, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE 35 (2003).

35 Krishna, *supra* note 27.

36 Wacks, *supra* note 28.

relates to the individual and which it would be reasonable to expect him to regard as intimate or sensitive and therefore to want to withhold or at least to restrict its collection, use, or circulation'.[37] If the right to privacy would be recognised by law, it would extend only over a limited, conventionally designated, area of information,[38]symbolic of the whole institution of privacy.[39] Hence, it can be argued that access to personal information is a necessary but not sufficient condition for it to be defined as falling within the scope of privacy. What is further required is that the information must be of an intimate and sensitive nature, such as information about a person's sexual proclivities, but the content may also differ considerably from society to society[40].

Attempts were also made to describe and evaluate the privacy term and its effect as a right which is protected equally for everyone in the eyes of law in the country of India. The right to privacy in India has derived itself from essentially two sources: the common law of torts and the constitutional law.[41] In common law, a private action for damages for unlawful invasion of privacy is maintainable. The printer and publisher of a journal, magazine or book are liable in damages if they publish any matter concerning the private life of the individual without such person's consent[42]. There are two exceptions to this rule: first, that the right to privacy does not survive once the publication is a matter of public record and, second, when the publication relates to the discharge of the official duties of a public servant, an action is not maintainable unless the publication is proved to be false, malicious or is in reckless disregard for truth[43].

Again under the constitutional law, the right to privacy is implicit in the fundamental right to life and liberty guaranteed by Article 21 of the Constitution. This has been interpreted to include the right to be let alone. The constitutional right to

---

37 *Id.* At 26.

38 Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 7 LAW & PHIL. 559 (1998).

39 Charles Fried, *Privacy*, 77 YALE L.J. 493 (1968).

40 *Id.*

41 There are also a few statutory provisions contained in the Code of Criminal Procedure, Sec. 327(1) (1973), the Indecent Representation of Women (Prohibition) Act, Sec. 3 and 4 (1980), The Medical Termination of Pregnancy Act, Sec. 7(1)(c) (1971), the Hindu Marriage Act, Sec. 22 (1955), the Special Marriages Act, Sec. 33 (1954), the Children Act, Sec. 36 (1960), and the Juvenile Justice Act, Sec. 36 (1968), all of which seek to protect women and children from unwarranted publicity.

42 This would include his family, marriage, procreation, motherhood, child-bearing, education etc.

43 Rachels, *supra* note 33.

privacy flowing from Article 21 must, however, be read together with the constitutional right to publish any matter of public interest, subject to reasonable restrictions. Furthermore, according to recommendations of *Venkata Challiah Commission*:

It is proposed that a new article, namely, article 21-B, should be inserted on the following lines:

> *21-B. (1) Every person has a right to respect for his private and family life, his home and his correspondence.*
>
> *(2) Nothing in clause (1) shall prevent the State from making any law imposing reasonable restrictions on the exercise of the right conferred by clause (1), in the interests of security of the State, public safety or for the prevention of disorder or crime, or for the protection of health or morals, or for the protection of the rights and freedoms of others*[44].

Unfortunately, even after passing of the ten years of recommendation by such an committee, the parliament could not dared to insert Art. 21 (B) as Right to Privacy and furthermore, another tragedy is that even Right to Privacy has not been included in Art. 19 (2) as reasonable restriction to Art.19 (1).

2.3. Conclusion

To conclude it can be stated that the law to privacy is recognition of the individual's right to be let alone and to have his personal space inviolate. The need for privacy and its recognition as a right is a modern phenomenon. It is the product of an increasingly individualistic society in which the focus has shifted from society to the individual where only describing or evaluating the term in general will not suffice any cause and hence is required to be studied as as right protected and promoted by the law of each state drawing its validity from the social pattern and values of a specific societal, political and economic compass. In early times, the law afforded protection only against physical interference with a person or his property. As civilization progressed, the personal, intellectual and spiritual facets of the human personality gained recognition and the scope of the law expanded to give protection to these needs. The essence of the law derives from a right to privacy, defined broadly as "the right to be let alone." It usually excludes personal matters or activities which may reasonably be of public interest, like those of celebrities or participants in newsworthy events.

---

[44] R. Rajagopal v. State of Tamilnadu, AIR 632 (6 SC 1994), 649-50.

Invasion of the right to privacy can be the basis for a lawsuit for damages against the person or entity violating the right.Hence, therefore this chapter has tried to understand and study the philosophical aspects behind the evolutionary principles of the term privacy and its development and stipulation of it gaining the status of a right . Further, the chapter has also concentrated on the definational aspects of the same to study the basic anonymity which revolves around the defination of privacy and it as a right and how is differs among different cultures and individuals.

CHAPTER 3

RIGHT TO PRIVACY: COMPARATIVE OUTLOOK AND INTERNATIONAL INSTRUMENTS

The better understanding of the theme of right to privacy and development of it requires a slight and brief visit of the international instruments validating or critisising the same and its evolution in various other countries along with the progress of the term in the Indian society. It can be stated that privacy is an inherent right of human being and its value can be traced from the biblical period. Almost the first page of the bible, writes *Prof. Milton R. Konwitz*, introduced us to the feeling of shame as violation of privacy. After Adam and Eve had eaten the fruit from the tree of knowledge, 'the eyes of both were opened, and they knew that they were naked; and they sewed fig leaves together and made themselves aprons'.[45] The frequent use of words like Ekant, Rahasaya, Tiraskarinee, Avagunthanvatee Naree and their synonyms in the Indian scriptures and classical literature, it cannot be said that privacy was alien to ancient Indian culture[46] too where it had a clutch over the idea since ancient period only. Even the importance of privacy and solitude is being attached to the process of mediation. Lord Shiva, while, in meditation, is said to have been disturbed by Kamdeva, the god of love and sex in the Indian mythology, who was burnt as a punishment therof when Lord Shiva opened his third eye[47]. The Gruhya-Sutras, Arthashastra and the epics of Ramayana and the Mahabharata talked about the sense of privacy in ancient society in India. The morality of Island based on the concept of Haya aims at inculcating a feeling of shyness in human nature and tries to develop it as a part of man's mental make-up so that it may serve as a strong moral deterrent against all evil inclination[48].

3.1. Right to Privacy and Comparative Outlook

Legal protections to privacy have existed in western countries for hundreds of years. Quite earlier the growth and development of the term right to privacy can be seen within the english legal system where the term was somewhat frequently been

---

45 Milton R. Konvitz, *Privacy and Law: Philosophical Prelude*, 31 LAW AND CONTEMPORARY PROBLEMS 272, 272-280 (1966).

46 ALAN F. WESTIN, PRIVACY IN INDIA, 47 (1994).

47 *Id.*

48 *Id.* at 70.

evaluated, upon its status as a right and the law protecting such a right and further, the justification it has in promoting and covering the term within the meaning of human right. In 1361, the *Justices of the Peace Act in England* provided for the arrest of peeping toms and eavesdroppers.[49] In 1765, British Lord Camden, striking down a warrant to enter a house and seize papers 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 the society, for papers are often the dearest property any man can have.' 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."[50]

One of the earliest cases in England, *Albert* v. *Strange* involved the unauthorized copying of etchings made by Queen Victoria and her husband for their private amusement. The etchings, which represented members of the Royal family and matters of personal interest, were entrusted to a printer for making impressions. An employee of the printer made unauthorized copies and sold them to the defendant who in turn proposed to exhibit them publicly. Prince Albert succeeded in obtaining an injunction to prevent the exhibition. The Court's reasoning was based on both the enforcement of the Prince's property rights as well as the employee's breach of confidence. This case is widely regarded as having inspired the development of the law of privacy in the United States[51].

Even as late as 1991, the law in England was found to be inadequate in protecting privacy. In that year, the Court of appeal decided *Kaye* v. *Robertson*. The case concerned a well-known actor who had to be hospitalized after sustaining serious head injuries in a car accident. At a time when the actor was in no condition to be interviewed, a reporter and a photographer from the Sunday Sport newspaper unauthorized gained access to his hospital room, took photographs and attempted to conduct an interview with the actor. An interlocutory injunction was sought on behalf

---

49 Thomas, Kendall, *Beyond the Privacy Principle*, 92 COLUM. L. REV. 1431, 1443-48 (1992); Yoshino, Kenji, Sodomy Laws: Law of the Bedroom, BOSTON GLOBE (Mar. 23, 2003), http://www.kenjiyoshino.Com/ articles/law_of_the_bedroom_sodomy_laws.pdf.

50 *Id.*

51 Albert v. Strange, 1 Mac & G 25: 41 ER 1171 (1849).

of the actor to prevent the paper from publishing the article which claimed that Kaye had agreed to give an exclusive interview to the paper. There being no right to privacy under the English law, the plaintiff could not maintain an action for breach of privacy. In the absence of such a right, the claim was based on other rights of action such as libel, malicious falsehood and trespass to the person, in the hope that one or the other would help him protect his privacy. Eventually, he was granted an injunction to restrain publication of the malicious falsehood. The publication of the story and some less objectionable photographs were, however, allowed on the condition that it was not claimed that the plaintiff had given his consent[52]. The remedy was clearly inadequate since it failed to protect the plaintiff from preserving his personal space and from keeping his personal circumstances away from public glare. The Court expressed its inability to protect the privacy of the individual and blamed the failure of common law and statute to protect this right.[53]

Various countries developed specific protections for the privacy in the centuries that followed. In 1776, the Swedish Parliament enacted the Access to Public Records Act that required that all government-held information be used for legitimate purposes. France prohibited the publication of private facts and set stiff fines for violators in 1858. The Norwegian criminal code prohibited the publication of information relating to person or domestic affairs in 1889.[54] It is pertinent to note here that in case of American legal system, "American law on privacy has evolved faster than the law in England.[55]

The innovative pontentials of the Courts has led to the mordern development of the term right to privacy in the United States.In USA, when the C onstitution and Bill of Rights were ratified. Neither statues nor common law rules established a right as such. And certainly there was no constitutional provision which clearly provided a vehicle for its inclusion. The common law with regard to trespass, assault, slander and libel, and

---

52 Kaye v. Robertson, FSR 62 (1991).

53 Hopefully, the Human Rights Act in 1998 which imposes a positive obligation to act in accordance with the European Convention on Human Rights will have a positive effect on the development of the law in the U.K.

54 *Supra* note 50.

55 Ironically, it was by borrowing from the English case-law and creatively interpreting it that the law in America developed. And yet, the law of privacy in England has lagged far behind, inviting serious criticism from commentators.

even nuisance (as applied to offensive noises and odors for example) could be said to have tangential reference to privacy, but this would offer a piecemeal approach rather than an argument based on a full-fledged right to privacy.[56]

The development of the law of privacy can be said to have originated with a law review article by Samuel D. Warren and Louis D. Brandeis in 1890. Out of a few fragments of common law, the authors invented a brand-new tort, the invasion privacy. Dean *Roscoe Pound* reportedly said that the article did nothing less than add a chapter to the law[57]. *Warren* and *Brandeis* began by noting new technological developments that were posing a potential threat to privacy and focused on how the common law could develop to protect the interest then called 'privacy'. the authors, however, did not spend much time setting forth a conceptual account of privacy[58]. *Warren* and*Brandeis* defined privacy as the "right to be let alone," a phrase adopted from judge *Thomas Cooley's* famous treatise on torts in 1880. *Cooley's* right to be let alone was, in fact, a way of explaining that attempted physical touching was a tort injury; he was not defined a right to privacy[59]. Warren and Brandeis's use of the phrase was consistent with the purpose of their article; to demonstrate that many of the elements of right to privacy existed within the common law[60].

The authors declared that the underlying principle of privacy was that of inviolate personality.[61] They noted that the value of privacy is found not in the right to take the profits arising from publication, but in the peace of mind or the relief afforded by the ability to prevent any publication at all.[62]*Warren* and *Brandies* observed that increasingly modern enterprise and invention have, through invasions upon privacy, subjected (an individual) to mental pain and distress, far greater than could be inflicted by mere bodily injury.[63] The authors noted that this type of harm was not typically protected by tort law. While the law of defamation protected injuries to reputations,

---

56 M. GLENN ABERNATHY, CIVIL LIBERTIES UNDER THE CONSTITUTION, 94 (1977).
57 *Id.* at 95.
58 Solove, *supra* note 16 at 1100.
59 Warren and Brandeirs, *supra* note 3 at 193.
60 Solove, *supra* note 16 at 1100.
61 Warren and Brandeirs, supra note 3 at 205.
62 *Id.* at 200.
63 *Id.* at 196.

privacy involved 'injury to the feelings', a psychological form of pain that was difficult to translate into the tort law of their times. Which focused more on tangible injuries.[64]

Nearly forty years later, when he was a justice on the Supreme Court, Brandeis wrote his famous dissent in *Olmstead* v. *United States*.[65] In *Olmstead*, the Court held that wiretapping was not a violation under the Fourth Amendment because it was not a physical trespeass into the homes. Brandeis fired off a dissent that was to become one of the most important documents for Fourth Amendment privacy law, stating that the Framers of the Constitution 'conferred, as against the government, the right to be let alone-the most comprehensive of rights and the right most valued by civilized men'.[66]Later, in *Brandeirs* article and his dissent in Olmstead have had a profound impact on the law of privacy and on subsequent theories of privacy. In *k* v. *United States*, the Court adopted Brandeis's view, overruling Olmstead.[67] In its Fourth Amendment jurisprudence, as well as its substantive due process protection of the right to privacy, the Court frequently has invoked Brandeis's formulation of privacy as "the right to be let alone.[68]

The formulation of privacy as the right to be let alone merely describes an attribute of privacy. Warren and Brandeis's aim was not to provide a comprehensive conception of privacy but instead to explore the roots of a right to privacy in the common law and explain how such right could develop. The article was certainly a profound beginning toward developing a conception of privacy[69]. In the years following the publication of the article, a law of privacy gradually developed by the statute and by the common law decision in the state Courts[70]. But it was not until 1965 that the US Supreme Court squarely held that the constitution contained at least a limited right to privacy[71]. The US Courts have developed privacy right on a constitutional basis. Various amendments of the American Constitution like 1st, 3rd, 4th and 5th containing

64 *Id.* at 197.
65 Olmstead v. United States, 277 U.S. 438 (1928).
66 *Id.* at 478.
67 Katz v. United States, 389 U.S. 347 (1967).
68 Solove, *supra* note 16 at 1101.
69 *Id.* at 1102.
70 Abernathy, *supra* note 56 at 95.
71 *Id.*

provisions protecting privacy interests has laid the necessary foundation for the Courts in this regard. These amendments mainly protect informational privacy[72].

The privacy regarding decisional privacy was protected mainly using the ninth amendment. Evolution of privacy as a constitutional right in America was through cases which fell in categories of (1) sexuality (2) search and seizure (3) eavesdropping (4) Data protection and press.[73] The great peculiarity of decisional privacy cases in America is their predominant focus on sexuality. Nothing is privacy cases has stressed that doctrine must gravitate around sexuality; nevertheless, it has. The American Courts or for that matter the judiciary has played a huge role in trasforming the role of the term privacy and its efficacy as a right where it first announced the right to privacy in a case involving a statute prohibiting use and distribution of contraceptive devices to married couples. In a later case the American Court invalidated a law criminalizing inter-racial marriage on the ground that it violated right to privacy.[74]

Further, in the case of US Supreme Court has found the rights of marriage, procreation, contraception, family relationships, child-rearing and education to be indefeasible fragments of the substantive right to privacy[75]. The fundamental choice of whether or not to beget a child forms the crux of this cluster of constitutionally protected decisions as 'decisions whether to accomplish or to prevent conception are amongstthe most private and sensitive'.[76] The substantive right to privacy has been described as a freedom in making certain kinds of intimate decisions[77]. Protection has not only been extended to certain kinds of decisions but also to certain kinds of places.[78]

In *Griswold v. Connecticut,* a majority of the Court indicated that the constitution creates 'Zones of privacy' which are beyond the scope of any legitimate search and held invalid the Connecticut law barring the use of any drug or instrument for contraceptive purposes. Justice Douglas, for the majority said: '*would we allow the*

---

72 Krishna, supra note 27 at 52.

73 *Id*. at 53.

74 *Id.*

75 Roe v. Wade, 410 US 113 (1973).

76 Meyer v. Nebraska, 262 US 390 (1923); Pierce v. Society of Sisters, 268 US 510 (1925); Prince v. Massachusetts, 321 US 158 (1944).

77 Carey v. Population Services International, 431 US 678, 685 (1977). See also Washington v. Glucksberg, 521 US 702 (1997) (dealing with the question of autonomy and suicide).

78 Security Recommendations for Stalking Victims.

police to search the sacred precincts of marital bedrooms for telltale signs of the use of contraceptives? The very idea is repulsive to the notions of privacy surrounding the marriage relationship.'[79]

Further, in the case of*Eisenstandt v. Baird*, the Court observed that if the right to privacy means anything it is the right of individual, married or single to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision whether to bear or beget a child[80].

Again in *Roe v. Wade*,[81]the Court struck down a Texas statute which prohibited almost all abortions. The Court's decision was based on the assumption that the right to abortion was part of a right of personal privacy. the Court observed:'*The right to privacy whether it be found in the 14th amendment concept of personal liberty and restrictions upon state action, as we feel it is or as the district Court determined, in the 9th amendment reservation of rights, is broad enough to compass a woman's decision whether or not to terminate her pregnancy.*'[82]

Similarly, in *Loving* v. *Virginia*, the US Supreme Court struck down a law which prevented interracial marriages.[83] However, the substantive right to privacy in the context of marriage suffered a substantial setback in *Bowers* v. *Hardwick* where the US Supreme Court denied privacy protection to homosexual activity.[84] The decision was reversed in 2003, in *Lawrence* v. *Texas*where Kennedy, J. found homosexuals to have the same rights as heterosexuals, beginning, in his eloquent judgment, with: '*Liberty protects the person from unwarranted government intrusions into a dwelling or other private places. In our tradition the State is not omnipresent in the home. And there are other spheres of our lives and existence, outside the home, where the State should not be a dominant presence. Freedom extends beyond spatial bounds. Liberty presumes an autonomy of self that includes freedom of thought, belief, expression, and certain intimate conduct.*'[85]

---

79 Griswold v. Connecticut, 381 U.S. 47 (1965).
80 Eisenstandt v. Baird, 405 U.S. 438 (1972).
81 *Supra* note 75.
82 *Id*. at 115.
83 Loving v. Virginia, 388 U.S. 1 (1967).
84 Bowers v. Hardwick, 478 US 186 (1986).
85 Lawrence v. Texas, 53hy9 US 558 (2003).

Again, in *Skinner* v. *Oklahoma*, the US Supreme Court struck down a statute which called for the sterilization of 'habitual criminals', thus ensuring their inherent right of procreation[86], while in *Stanley* v. *Georgia*, the possession of obscene material in a man's house was condoned for the reason:if the First Amendment means anything, it means that a State has no business telling a man, sitting alone in his own house, what books he may read or what films he may watch. Our whole constitutional heritage rebels at the thought of giving Government the power to control men's minds.[87]

The constitutional right to privacy, however, is not an absolute right. It can bee curtailed on the ground of compelling social interest or in the interest of basic competing right of other individuals.In America, the 4th and 5th amendments provide the necessary safeguards against arbitrary search[88].After a very long debate the US Supreme Court adopted the wider approach and overruled the narrower approach of its own Augustus fraternity in *Kats* v. *United States"*.Stewart J. wrote that although a closely divided Court supposed in Olmstead that surveillance without any trespass and without any seizure of any material object fell outside the ambit of the constitution, we have since departed from the narrow view on which that decision rested. Indeed, we have expressly held that fourth amendment governs not only the seizure of tangible items but extends as well to the recording or oral statements, overheard without any technical trespass.[89]

It is pertinent to mention here that along with the protection of the privacy rights in sectors like that of marriage, procreation, contraception, family relationships, child-rearing, education, search and seizure and many such others, information or data protection privacy also falls in one of the many important sector which the government through its positive actions should try to protect and promote.In most of the countries of the world, the judiciary has played a great role in protecting the privacy rights of an individual through interpretating the laws as it is or in the form where such a right could be established and then be protected. But the intrusion and violation of such a right is quite frequentby various governmental and non-governmental agencies, justifying the

86 Skinner v. Oklahoma, 316 US 535 (1942).
87 Stanley v. Georgia, 394 US 557 (1969).
88 Krishna, *supra* note 27 at 55.
89 Kats v. United States, 389 U.S. 347 (1967).

act in the name of national interest and hence thereby gathering the data/ information of individuals with or without their consent.And hence therefore, the need of specific data protection laws in states are highly required to prevent the true essence of privacy as a fundamental right.

Information privacy law or data protection laws prohibit the disclosure or misuse of information about private individuals. Over 80 countries and independent territories, including nearly every country in Europe and many in Latin America and the Caribbean, Asia, and Africa, have now adopted comprehensive data protection laws[90]. While talking of the violation and intrusion of the right to privacy, the government is not the only entity which may pose a threat to data privacy. Other citizens, and private companies most importantly, may also engage in threatening activities, especially since the automated processing of data became widespread. Hence, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data was concluded within the *Council of Europe* in 1981. This convention obliges the signatories to enact legislation concerning the automatic processing of personal data, which many duly did[91].The European Union has the General Data Protection Regulation, in force since May 25, 2018[92]. The right to data privacy is relatively heavily regulated and actively enforced in Europe. The European Court of Human Rights has given Article 8 of ECHR (which will be duly discussed below) a very broad interpretation in its jurisprudence. According to the Court's case law the collection of information by officials of the state about an individual without their consent always falls within the scope of Article 8. Thus, gathering information for the official census, recording fingerprints and photographs in a police register, collecting medical data or details of personal expenditures and implementing a system of personal identification has been judged to raise data privacy issues[93].

On the other hand the United States is notable for not having adopted a comprehensive information privacy law where the data privacy is not highly legislated

---

90 Greenleaf Graham, *Global Data Privacy Laws: 89 Countries, and Accelerating*, Social Science Electronic Publishing, 98 QUEEN MARY SCHOOL OF LAW LEGAL STUDIES (2012).

91 *Id.*

92 Dativa, *Adopting a Virtual Data Protection Officer*, (June 11, 2018) https://www.dativa.com/virtual-dpo/.

93 European Convention on Human Rights, (04.11.1950) http://www.hrcr.org/docs/Eur_ Convention/euroconv3.html (03.09.1953).

or regulated in USA, but rather having adopted limited sectoral laws[94] in some areas which plays the role of protecting the privacy rights of the public, for instance, the *Health Insurance Portability and Accountability Act* of 1996 (HIPAA), the *Children's Online Privacy Protection Act* of 1998 (COPPA), Right to Know Act (California Bill AB 1291)[95]and the *Fair and Accurate Credit Transactions Act* of 2003 (FACTA), are all examples of U.S. federal laws with provisions which tend to promote information flow efficiencies[96]. But it is pertinent to mention here that the US government provides with the *Privacy Act* of 1974, which protects records held by US Government agencies and requires them to apply basic fair information practices. Like the Indian Constitution, there is no explicit right to privacy in the US Constitution. However, US Courts have interpreted the right to privacy to be included in the US Constitution.[97]

Again, in the United Kingdom the *Data Protection Act* 1998 (Information Commissioner) implemented the EU Directive on the protection of personal data. It replaced the Data Protection Act 1984. The 2016 General Data Protection Regulation supersedes previous Protection Acts[98]. In Switzerland, the right to privacy is guaranteed in article 13 of the Swiss Federal Constitution. The Swiss Federal Data Protection Act (DPA) and the Swiss Federal Data Protection Ordinance (DPO) entered into force on July 1, 1993. The latest amendments of the DPA and the DPO entered into force on January 1, 2008[99]. Also, in Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) went into effect on 1 January 2001, applicable to private

---

94 These laws are based on Fair Information Practice that was first developed in the United States in the 1970s by the Department for Health, Education and Welfare (HEW). The basic principles of data protection are for all data collected there should be a stated purpose, information collected by an individual cannot be disclosed to other organizations or individuals unless specifically authorized by law or by consent of the individual, records kept on an individual should be accurate and up to date, there should be mechanisms for individuals to review data about them, to ensure accuracy. This may include periodic reporting, data should be deleted when it is no longer needed for the stated purpose, transmission of personal information to locations where "equivalent" personal data protection cannot be assured is prohibited, some data is too sensitive to be collected, unless there are extreme circumstances (e.g., sexual orientation, religion).

95 Bonnie Lowenthal, *AB-1291 Privacy: Right to Know Act of 2013: disclosure of a customer's personal information*,(June16,2018)http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?billid=201 32014 0AB129.

96 Frontier Technology, *The difference between EU and US data laws*, (June 116, 2018) http://www.frontiertechnology.co.uk/about-us/news/differences-between-eu-and-us-data-laws/.

97 Marc Rotenberg, *The Privacy Law Sourcebook*, EPIC 1999, (June 20, 2018), http://www.epic.org/bookstore/pls.

98 Bonnie, s*upra* note 95.

99 *The Federal Council's Message to Parliament*, 19 BBl 2101, https://www.admin.ch/opc/de/federal-gazette/2003/2101.pdf (last updated 2003).

bodies which are federally regulated. All other organizations were included on 1 January 2004. The PIPEDA brings Canada into compliance with EU data protection law[100], hence making the every possible way through which the individual's data information can be protected and therefore securing the right to privacy in concrete.

3.2. International recognition of Right to Privacy

Privacy is considered as an essential to who we are as human beings, and we make decisions about it every single day. It notably gives us a space to be ourselves without judgement, allows us to think freely without discrimination, and is an important element of giving us control over who knows what about us. In most the nations today, privacy is the one which is measured and qualified as a fundamental human right and has been interpretated and alloted the status of a right, violation of which can be protected in the Court of law. Hence, the right to privacy is enunciated in all major international and regional human rights instruments.

Internationally the right to privacy has been protected in a number of conventions. For instance, the Universal Declaration of Human Rights, 1948 (UDHR) under Article 12 provides that: "*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*."[101]Further, Article 19 of the UDHR declares that "*Everyone has the right to freedom of opinion and expression: the right includes freedom to hold opinion without interference, and to seek, and receive and impart information and ideas through any media and regardless of frontiers*."[102]

The UDHR protects any arbitrary interference from the State to a person's right to privacy. Similarly, International Covenant on Civil and Political Rights, 1976 (ICCPR) under Article 17 imposes the State to ensure that individuals are protected by law against "*arbitrary or unlawful interference with his privacy, family, home or*

---

100 *Protecting and Promoting Privacy Rights*, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, https://www.priv.gc.ca/en/ (last updated February 16, 2014).

101 Universal Declaration of Human Rights, art. 12, Dec. 12, 1948, Res. 217 A, Sess. 3rd, 183rd Plenary meeting, U.N. Document A/RES/ 217 (III).

102 Universal Declaration of Human Rights, art. 19, Dec. 12, 1948, Res. 217 A, Sess. 3rd, 183rd Plenary meeting, U.N. Document A/RES/ 217 (III).

correspondence, nor to unlawful attacks on his honor and reputation."[103]Thus, ensuring that States enact laws to protect individual's right to privacy. India has ratified the above conventions. The ratification of the Conventions mandates the State to take steps to enact laws to protect its citizens. Although, human right activists have periodically demanded that the State take adequate measures to protect human rights of the vulnerable in society, the right to privacy has received little attention.[104]

Similarly, Article 16 of the UN Convention on the Rights of the Child (CRC), 1989 provides protection to a minor from any unlawful interference to his/her right to privacy and imposes a positive obligation on States who have ratified the convention to enact a law protecting the same. India does have safeguards in place to protect identity of minors, especially, juveniles and victims of abuse. However, there are exceptions when the law on privacy does not apply even in case of a minor.[105]

Article 8 of the European Convention on Human Rights, 1950[106] reads as follows:

> *"(1) Everyone has the right to respect for his private and family life, his home and his correspondence.*
> *(2) There shall be no interference by a public authority with the exercise of this right, except such as is in accordance with law and is necessary in a democratic society in the interests of national security, public safety, for the prevention of disorder and crime or for the protection of health or morals."*[107]

The right to privacy is also included in:

- Article 14 of the United Nations Convention on Migrant Workers, 1994;
- Article 10 of the African Charter on the Rights and Welfare of the Child, 1990;
- Article 4 of the African Union Principles on Freedom of Expression (the right of access to information), 2002;
- Article 11 of the American Convention on Human Rights, 1969;
- Article 5 of the American Declaration of the Rights and Duties of Man, 1948;
- Articles 16 and 21 of the Arab Charter on Human Rights, 1994;

---

103 International Covenant on Civil and Political Rights, art. 17, March 23, 1976, Res. 2200 A, U.N. Document A/RES/ 21/ 2200.

104 *Id.*

105 UN Convention on the Rights of the Child, art. 16, Nov. 20, 1989, Res. 44/25.

106 Bonnie, s*upra* note 95.

107 *Id.*

- Article 21 of the ASEAN Human Rights Declaration, 2012; and

Over 130 countries have constitutional statements regarding the protection of privacy, in every region of the world. An important element of the right to privacy is the right to protection of personal data. While the right to data protection can be inferred from the general right to privacy, some international and regional instruments also stipulate a more specific right to protection of personal data, including:

- the OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,
- the Council of Europe Convention 108 for the Protection of Individuals with Regard to the Automatic Processing of Personal Data,
- a number of European Union Directives and its pending Regulation, and the European Union Charter of Fundamental Rights,
- the Asia-Pacific Economic Cooperation (APEC) Privacy Framework 2004, and
- the Economic Community of West African States has a Supplementary Act on data protection from 2010[108].

3.3. Role of Judiciary in recognising the Right to Privacy in India.

India being a signatory to many of the aforesaid international instruments like that of UDHR, ICCPR, etc., the judiciary and the government has tried to a great extent to justify the term privacy as a right and to promote and protect it from getting violated. Though there are different laws or provisions which indirectly speaks for the protection of the right to privacy in India,[109] there lacks a specific privacy law or for that matter a data privacy or information protection law through which such right can be regulated. In India, ones right to privacy has to wait to be sheltered through judicial interpretation of the existing laws, which makes it more endangered of getting violated. The debate over privacy issue focus primarily on protecting the domestic privacy rights of citizens within national border. The right to privacy is an independent and indistinctive conceptthat oriented in the field of Tort Law, under which the new cause of action for

108 JUSTICE YATINDRA SINGH, CYBER LAWS 156 (Universal Law Publishing, 6th ed. 2016).

109 The privacy specific laws will be discussed broadly in the next chapter.

damage resultingfrom unlawful invasion of privacy was recognized[110]. It is perhaps still a debatable issue to tellwhetherprivacy, however how great a value, can function as a constitutional concept[111].

Since, the Indian Constitution does not talk about this right specifically, it was developed by the various judicial pronouncements made on this subject matter by the Hon'ble Supreme Court. In 1965, the Supreme Court of India heard and decided *State of U.P.*v. *Kaushaliyal and others*, a case which involved the question of whether women who are engaged in prostitution can be forcibly removed from their residences and places of occupation, or whether they were entitled, along with other citizens of India, to the fundamental right to move freely throughout the territory of India, and to reside and settle in any part of the territory of India under Article 19(l)(d) and (e) of the Constitution of India. In other words, did these women possess an absolute right of privacy over their decisions in respect to their occupation and place of residence? In its decision, the Supreme Court denied them this right holding that the activities of a prostitute in a particular area are so subversive of public morals and so destructive of public health that it is necessary in public interest to deport her from that place. In view of their 'subversiveness', the statutory restrictions imposed by the Suppression of Immoral Traffic Act on prostitutes, were upheld by the Court as constitutionally-permissible 'reasonable restrictions' on their movements[112].

> "The legal alibis that the State employs to justify its infringement of our privacy are numerous, and range from 'public interest' to 'security of the state' to the 'maintenance of law and order'. The statutory venues of deprivation of privacy by the state being many, strictly, any statute that imposes any restriction on movement, or authorizes the search or examination of any residence or book, or the interception of communication may be read as a violation of a privacy right, tracking each of these down would not only be an impossible exercise, but also contribute little to the analytical exercise we are attempting here. Instead, in this chapter we only list provisions from a few statutes that are the familiar instruments by which the state impinges on our privacy. This is done with the limited object of arriving at a rough inventory of the common technologies which the state employs to impinge on our privacy. Even if intrusions into our privacy are statutorily authorised, these statutes must withstand constitutional scrutiny.

110 2 BASU, DURGA DAS, COMMENTARY ON THE CONSTITUTION OF INDIA 4772 (Lexis Nexis, 3rd ed. 2016).

111 *Id.*

112 State of U.P. v. Kaushaliyal and others, AIR 416 (SC 1964).

> Although not specifically referenced in the Constitution, the Right to Privacy is considered a 'penumbral right' under the Constitution i.e. a right that has been declared by the Supreme Court as integral to the Fundamental Right to Life and Liberty. In addition, although no single statute confers a cross-cutting 'horizontal' right to privacy various statutes contain provisions which either implicitly or explicitly preserve this right. The following provisions provide an overview of both constitutional and statutory safeguards to privacy in India. Hence, though the Indian Constitution does not contain an explicit reference to a Right to Privacy, this right has been read in to the constitution by the Supreme Court as a component of two Fundamental Rights: the right to freedom under Article 19 and the right to life and personal liberty under Article 21. It would be instructive to provide a brief background to each of these Articles before delving deeper into the privacy jurisprudence expounded by the Courts under them"[113].

Later in the caseof *Kharak Singh* v. *State of U.P*, where the the question for consideration in this case was whether 'surveillance' under Chapter XX of the U.P. Police Regulations constituted an infringement of any of the fundamental rights guaranteed by Part III of the Constitution. Regulation 236(b) which permitted surveillance by 'domiciliary visits at night' was held to be violative of Article 21.The meanings of the word life and the expression personal liberty in Article 21 were elaborately considered by this Court in Kharak Singh's case. This casebrought the question of privacy in India and also became a pedestal through which Supreme Court established that right to privacy does not form part of the guaranteed rights given by the Constitution to its citizens, but the minority opinion of the case was much inclined towards determining this new right under the expression Personal Liberty in Article 21 of the Constitution of India. This judgment although not conclusive, but it opened up the doors for debate over the profound right[114].

In 1972, the Supreme Court decided one of its first cases on the constitutionality of wiretapping. In *R. M. Malkani* v. *State of Maharashtra* the petitioner's voice had been recorded in the course of a telephonic conversation where he was attempting blackmail. He asserted in his defence that his right to privacy under Article 21 had been violated. The Supreme Courtdeclined his plea holding that the telephonic conversation of an innocent citizen will be protected by Courts against wrongful or high handed' interference by tapping the conversation. The protection is not for the guilty citizen

---

113 D.K. SINGH, V. N. SHUKLA'S CONSTITUTION OF INDIA (Eastern Book Company, Delhi, 7th ed. 1982).

114 Kharak Singh v. State of U.P, AIR 1925 (SC 1963).

against the efforts of the police to vindicate the law and prevent corruption of public servants.[115]

The further development of this issue was undertaken in the case of *Govind* v. *State of Madhya Pradesh* whose decision was given after referring to a U.S Court judgment in *Griswold* v. *State of Connecticut*[116]. Here, the Court was evaluating the constitutional validity of Regulations 855 and 856 of the Madhya Pradesh Police Regulations which provided for police surveillance of habitual offenders which including domiciliary visits and picketing of the suspects. The Supreme Court desisted from striking down these invasive provisions and held that right to privacy was implied in Article 19(1)(a) and Article 21, but the right was not of the absolute nature and any intrusion done by the state was permitted to the level that it was based on reasonable materials to support its action. Although the principle laid down in the above case is now encountering friction but still the judgment gave recognition to the privacy rights, mostly in the minimum possible way i.e. in an implied manner[117]. The development was further taken up in the case of *R.Rajgopal* v. *State of Tamil Nadu*[118]. The case was related to the publication by a newspaper of the autobiography of Auto Shankar who had been convicted and sentenced to death for committing six murders. In the autobiography, he had commented on his contact and relations with various high-ranking police officials-disclosures which would have been extremely sensational. Sometime before the publication, he appears to have been induced to write a letter disclaiming his authorship of the autobiography. On this basis, the Inspector General of Prisons issued a letter forbidding the newspaper from publishing the autobiography claiming, inter alia, that the publication of the autobiography would violate the prisoner's privacy. Curiously, neither Shankar himself, nor his family were made parties to this petition. The Court decided to presume, somewhat oddly, that he had 'neither written his autobiography' nor had he authorised its publication. The Court then proceeded on this assumption to enquire whether he had any privacy interests that would be breached by unauthorised publication of his life story. The right of privacy of citizens was dealt with by the Supreme Court in the following terms:-

---

115 R. M. Malkani v. State of Maharashtra, AIR 157 (SC 1973); 1973 SCR (2) 417.
116 *Supra* note 79.
117 Govind v. State of Madhya Pradesh, AIR 1376 (SC 1975).
118 *Supra* note 44.

1. The right to privacy is implicit in the right to life and liberty guaranteed to the citizens of this country by Article 21. It is a 'right to be let alone'. A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, childbearing and education among other matters. None can publish anything concerning the above matters without his consent - whether truthful or otherwise and whether laudatory or critical. If he does so, he would be violating the right to privacy of the person concerned and would be liable in an action for damages. Position may, however, be different, if a person voluntarily thrusts himself into controversy or voluntarily invites or raises a controversy.

2. The rule aforesaid is subject to the exception, that any publication concerning the aforesaid aspects becomes unobjectionable if such publication is based upon public records including Court records. This is for the reason that once a matter becomes a matter of public record, the right to privacy no longer subsists and it becomes a legitimate subject for comment by press and media among others. We are, however, of the opinion that in the interests of decency (Article 19(2)) an exception must be carved out to this rule, viz., and a female who is the victim of a sexual assault, kidnap, abduction or a like offence should not further be subjected to the indignity of her name and the incident being publicised in press/media.[119]

In this particular case Supreme Courton the above reasoning upheld that the newspaper's right to publish Shankar's autobiography, even without his consent or authorisation, to the extent that this story was able to be pieced together from public records. The Courtfinally asserted on the point that in recent times the right to privacy has acquired Constitutional Status. It is implicit in the right to life and liberty guaranteed to the citizens[120]. A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, information given to public or private authority and education[121].

---

119 M.P JAIN, INDIAN CONSTITUTIONAL LAW 1237 (LexisNexis ButterworthsWadhwa Nagpur, 6th ed. 2012).

120 *Id.*

121 Although the constitution of the U.S.A does not explicitly mentions any right of privacy, the U.S Supreme Court recognizes that a right of personal privacy, or a guarantee of certain areas or zones of privacy, does exist under the Constitution and the roots of that right can be found in the first amendment followed by the fourth and the fifth amendment.

Furthermore, as per the judgment of *PUCL* v. *Union of India*, a public interest litigation, in which the Court was called upon to consider whether wiretapping was an unconstitutional infringement of a citizen's right to privacy. The case was filed in light of a report brought out by the Central Bureau of Investigation on the 'Tapping of politicians' phones' which disclosed several irregularities in the tapping of telephones. On the concept of the 'right to privacy' in India, the Court made the following observations:

> "The right privacy by itself has not been identified under the Constitution. As a concept it may be too broad and moralistic to define it judicially. Whether right to privacy can be claimed or has been infringed in a given case would depend on the facts of the said case.' However, the Court went on to hold that 'the right to hold a telephone conversation in the privacy of one's' home or office without interference can certainly be claimed as right to privacy'. This was because 'conversations on the telephone are often of an intimate and confidential character. Telephone conversation is an important facet of a man's private life. Right to privacy would certainly include telephone-conversation in the privacy of one's home or office. Telephone-tapping would, thus, infract Article 21 of the Constitution of India unless it is permitted under the procedure established by law."[122]

This case made two important contributions to communications privacy jurisprudence in India, the first was its rejection of the contention that 'prior judicial scrutiny' should be mandated before any wiretapping could take place. Instead, the Court accepted the contention that administrative safeguards would be sufficient. Secondly, the Court prescribed a list of procedural guidelines, the observance of which would save the wiretapping power fromunconstitutionality. In 2007, these safeguardswere formally incorporated into the Rules framed under the Telegraph Act.[123]

Further, it can be stated that the validity was also implicitly provided by the very Preamble of the Constitution to right to Privacy in India. Theterm Fraternity is explained by adding to it as assuring the dignity of the individual, andthe dignity of an

---

122 PUCL v. Union of India, AIR 568 (SC 1997).

123 Rule 419A of the Telegraph Rules stipulates the authorities from whom permission must be obtained for tapping, the manner in which such permission is to be granted and the safeguards to be observed while tapping communication. The Rule stipulates that any order permitting tapping of communication would lapse (unless renewed) in two months. In no case would tapping be permissible beyond 180 days. The Rule further requires all records of tapping to be destroyed after a period of two months from the lapse of the period of interception.

individual is already covered under the umbrella of Article 21[124]. The case of *Suresh Kumar Koushal and Others*. v. *Naz Foundation and Others*[125] have specially talked about the issue and Hon'ble Supreme Court have said that a test have to be satisfied while judging the constitutionality of a provision which purports to restrict or limit the right to life and liberty, including the right to privacy, dignity and autonomy as envisaged under Article 21[126]. This point was even raised and used by the respondent of the case in his arguments; the right to equality under Article 14 and the Right to dignity and Privacy under Article 21 are interlinked and must be fulfilled for other constitutional rights to be truly effectuated.[127] Thus, even without a direct mention of such a profound right in the list of the fundamental rights provided in the Constitution of India, the Hon'ble Supreme Court have managed several times to establish the right and have asserted in its prior pronouncements that right to privacy now holds a constitutional status, and with the backing of preamble in its favor Right to Privacy have held a further strong foundation to be passed as a legislation and become an absolute right for the citizens of India[128].

3.4. Conclusion

To conclude, it can be stated that the privacy right in India in its very foundation a limited right rather than an absolute right, a limited right which is existing in the reasonable interpretation of the Indian judiciary trying to protect and promote the privacy rights of the people of India. This very nature of the peivay rights in India makes the right wobbly and without any assurance, since it is frequently made to yield to a range of conflicting interestslike that of rights of paternity, national security, maintenance of law and order, etc. which happen to have a more pronounced standing in law, compared to that of a right which is limited in its form.It is our purpose to consider whether the existing law affords a principle which can properly be invoked to protect the privacy of an individual; and, if it does, what the nature and extent of such protection is. And to understand the duty of the state to enact an absolute law to prevent any such intusion and violation of the privacy rights which may be in the form of

124 P.M. BAKSHI, THE CONSTITUTION OF INDIA (Delhi: Universal Law Publication, 2009).
125 Suresh Kumar Koushal and Others. v. Naz Foundation and Others, SCC (Cri. 1) (4 SC 2013).
126 AbhinavChandrachud, *The Substantive Right to Privacy: Tracing the Doctrinal Shadows of the Indian Constitution,* 3 S.C.C. (Jour.) 31 (2006).
127 Jain, *supra* note 119.
128 *Id.*

personal or data information or in the way or choice one wants to live his/her life. For instance, it is to be noted that over 100 countries now have some form of privacy and data protection law. However, it is all too common that surveillance is implemented without regard to these protections. That's one of the reasons why international privacy instruments are around to make sure that the powerful institutions such as governments and corporations don't abuse laws and loopholes to invade your privacy. The right to privacy, therefore, is not an absolute right and does not apply uniformly to all situations and all class of persons[129]. But keeping in mind or looking into the progress and development of the international instruments and judicial trend, there should be a separate positive law enacted, giving status to the term privacy as a right and protection from the law.

[129] Chandrachud, *supra* note 127.

CHAPTER 4

LAWS RELATING TO RIGHT TO PRIVACY IN INDIA: AN ANALYSIS

The delivery of the judgment of *Maneka Gandhi* v. *Union of India* had enormously increased the ambit of Art. 21 of the Indian Constitution[130] so that it could implicitly include centain fundamental rights to the humans which are not drescribed in the express provisions by the legislature in the form of an Act. And hence therefore, right to privacy is one of those fundamental rights which has been progressed by the Indian jurisprudence alongside the Apex Court of the land within the meaning of Art. 21 of the Constitution.An attempt at defining privacy is of no use if the levels of abstraction do not translate into concrete specifics. Broadly speaking, privacy law deals with freedom of thought, control over one's body, peace and solitude in one's home, control of information regarding oneself, freedom from surveillance,[131] protection from unreasonable search and seizure,[132] and protection of reputation,and many such others[133]. There are various Indian laws in actions, certain provisions of which speaks about the specific protection of the privacy rights of people, some of which will be dicussed as follows. But the question remains intact in the need of a positive statutory enaction of a law/Act, which gives explicit entitlement to the term privacy as a right and protection from the law.

4.1. Study of the Privacy of Communications

Freedom in communication is one of the most basic essential of one's privacy rights where one imparts or exchange any information by speaking, writing or using

130 Hereafter referred as 'Constitution'.

131 The early Indian privacy cases dealt exclusively with police surveillance of habitual criminals. See e.g. Kharak Singh v. State of U.P., AIR 1295 (SC 1963) (challenging Chapter XX of the U.P. Police Regulations which placed possible criminals under surveillance); Gobind v. State of M.P., AIR 148 (2 SC 1975) (challenging the validity of Regulations 855 and 856 of the M.P. Police Regulations, which permitted the police to keep an uncomfortable surveillance on individuals suspected of perpetrating crime).

132 The Fourth Amendment of the US Constitution provides a safeguard from unreasonable search and seizure, and no search can be carried out without a warrant issued on probable cause. The Supreme Court has not allowed Fourth Amendment developments to percolate into the Indian Constitution. See M.P. Sharma v. Satish Chandra, SCC 300 (SC 1954) (rejecting the premise that search and seizure violates the principle of self-incrimination embedded in Article 20(3) of the Constitution). But see District Registrar and Collector v. Canara Bank, SCC 496 (1 SC 2005) (finding the Andhra Pradesh Amendment to Stamp Act, Sec. 73 (1899), to be unconstitutional since it permitted search and seizure on private premises).

133 Solove, *supra* note 16.

some other medium, and hence state is at the utmost duty to protect such communications from getting intruded or violated by any state or private mechanisms. India in this regard has adopted many national and state legislation, within which provisions are reflected protecting the communicating rights of the people under the head of right to privacy, some of which are evaluated below.

4.1.1. Communication Laws

All laws dealing with mediums of inter-personal communication like that of post, telegraph and telephone and email, contain similarly worded provisions permitting interception underspecified conditions. Thus, Section 26 of the *India Post Office Act* confers powers of interception of postal articles for the 'public good'. According to this section, this power may be invoked 'on the occurrence of any public emergency, or in the interest of the public safety or tranquillity'. The section further clarifies that 'a certificate from the State or Central Government' would be conclusive proof as to the existence of a public emergency or interest of public safety or tranquillity[134].

Similarly, Section 5(2) of the *Telegraph Act* authorizes the interception of any message:

> *"a) on the occurrence of any public emergency, or in the interest of the public safety; and*
> *b) if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offence"*[135].

Most recently, Section 69 of the *Information Technology Act* 2008 contains a more expanded power of interception which may be exercised "when they (the authorised officers) are satisfied that it is necessary or expedient' to do so in the interest of:

a) sovereignty or integrity of India,

b) defence of India,

c) security of the State,

d) friendly relations with foreign States, or

---

134 India Post Office Act, Sec. 26 (1898).

135 The Indian Telegraph Act, Sec. 5 (1885).

e) public order, or

f) preventing incitement to the commission of any cognizable offence relating to above,or

g) for investigation of any offence"[136].

The plain reading of these sections, there appears to be a gradual loosening of standards from the *Post Office Act* to the latest *Information Technology Act (IT Act)*. The *Post Office Act* requires the existence of a 'state of public emergency' or a 'threat to public safety and tranquillity' as a precursor to the exercise of the power of interception. This requirement is continued in the *Telegraph Act* with the addition of a few more conditions, such as expediency in the interests of sovereignty, etc. Under the most recent *IT Act*, the requirement of a public emergency or a threat to public safety is dispensed with entirely. Here, the government may intercept merely if it feels it 'necessary or expedient'[137].

In *Hukam Chand Shyam Lal* v. *Union of India and others*, the Supreme Court was required to interpret the meaning of 'public emergency'. Here, the Court was required to consider whether disconnection of a telephone could be ordered due to an 'economic emergency'. The Government of Delhi had ordered the disconnection of the petitioner's telephones due to their alleged involvement, through the use of telephones, in (then forbidden) forward trading in agricultural commodities. According to the government, this constituted an 'economic emergency' due to the escalating prices of food. Declining this contention, the Supreme Court held that: a 'public emergency' within the contemplation of this section is one which raises problems concerning the interest of the public safety, the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or the prevention of incitement to the commission of an offence[138].

Economic emergency is not one of those matters expressly mentioned in the statute. Mere 'economic emergency' as the high Court calls it may not necessarily

---

136 Information Technology Act, Sec. 65 (2008).

137 SubhajitBasu, *Policy-making, Technology and Privacy in India*, 6 THE INDIAN JOURNAL OF LAW AND TECHNOLOGY 70, 65-88 (2010).

138 Hukam Chand ShyamLal v. Union of India and others, AIR 789 (SC 1976), 1976 SCR (2)1060, (1976) 2 SCC 128.

amount to a 'public emergency' and justify action under this section unless it raises problems relating to the matters indicated in the section. In addition the other qualifying term, 'public safety' was interpreted in an early case by the Supreme Court to mean 'security of the public or their freedom from danger. In that sense, anything which tends to prevent dangers to public health may also be regarded as securing public safety. The meaning of the expression must, however, vary according to the context.'[139]

Thus, the government just cannot encroach one's right to privacy in the name of public emergency or safety. Though both the concepts do act as a limit on one's right to privacy, but the government before making the impringe must demonstrate their existence to the satisfaction of the Court, failing to which make their actions illegal. However, as mentioned, even these requirements have been dispensed with in the case of electronic communications falling under the purview of the Information Technology Act where sweeping powers of interception have been provided extending from matters affecting the sovereignty of the nation, to the more mundane 'investigation of any offence'[140].

4.1.2. Privileged Communications

In addition to laying down procedural safeguards which restrict the conditions under which our communication may be intercepted, the law also safeguards our privacy in certain contexts by taking away the evidentiary value of certain communications. Thus, for instance, under the *IndianEvidence Act*, communications between spouses and communications with legal advisors are accorded a special privilege.Section 122 of the *Indian Evidence Act* forbids married couples from disclosing any communications made between them during marriage without the consent of the person who made it, where there are certain exceptions to the provision asthat of 'any communication made in furtherance of any illegal purpose and any fact observed by any barrister, pleader, attorney or vakil, in the course of his employment as such showing that any crime or fraud has been committed since the commencement of his employment'. This however, does not apply in suits 'between married persons,

139 RomeshThappar v. The State of Madras, AIR 124 (SC 1950), 1950 SCR 594.
140 *Id.*

or proceedings in which one married person is prosecuted for any crime committed against the other.'[141] This rule was applied in a case before the Kerala High Court, *T.J. Ponnenvs M.C.* v. *Varghese* where a man sued his son-in-law for defamation based on statements about him written in a letter addressed to his daughter. The trial Court held that the prosecution was invalid since it was based on privileged communications between the couple. This was upheld by the high Court. The petitioner had attempted to argue that it was immaterial how he gained possession of the letter. The high Court disagreed with this contention holding that this would defeat the purpose of Section 122[142].

Similarly, Section 126 forbids 'barristers, attorneys, pleaders or vakils' from disclosing, without their client's express consent 'any communication made to him in the course and for the purpose of his employment as such barrister, pleader, attorney or vakil or to state the contents or condition of any document with which he has become acquainted in the course and for the purpose of his professional employment or to disclose any advice given by him to his client in the course and for the purpose of such employment.'[143]

Furthermore, Section 127 extends the scope attorney-client privilege to include any interpreters, clerks and servants of the attorney or barrister. They are also not permitted to disclose the contents of any communication between the attorney and her client[144]. Further, Section 129 enacts a reciprocal protection and provides that clients shall not be compelled to disclose to the Court any 'confidential communication which has taken place between him and his legal professional adviser.'[145] Again, Section 131 of the Evidence Act further cements the legal protection afforded to married couples, attorneys and their clients by providing that 'No one shall be compelled to produce documents in his possession, which any other person would be entitled to refuse to produce if they were in his possession' unless that person consents to the production of such documents[146]. These privileges do not limit the ability of the

141 Indian Evidence Act, Sec. 122 (1872).
142 Ponnenvs M.C. v. Varghese, AIR 228 (Ker. 1967), 1967 Cri.L.J. 1511.
143 Indian Evidence Act, Sec. 126 (1872).
144 Indian Evidence Act, Sec. 127 (1872).
145 Indian Evidence Act, Sec. 129 (1872).
146 Indian Evidence Act, Sec. 131 (1872).

state to intercept communications, they merely negate the evidentiary value of any communications so intercepted.[147]

4.2. Privacy of the Home: Search and Seizure Provisions

What are the circumstances under whih the State can invade the privacy of our homes is a significant question.Technically, any law that authorizes 'search and seizure' can be said to authorize an invasion of our privacy. Many laws permit searches, for various grounds ranging from the *Income Tax Act* which authorizes searches to recover undisclosed income, to the *Narcotics Act* which prescribes a procedure to search and seize drugs, to the *Excise Act* and the *Customs Act* which do so in order to discover goods that are manufactured or imported in violation of those respective statutes. Again, under the *Code of Criminal Procedure (Cr.P.C)*; 1973, it provides that a house or premises may be searched either under a search warrant issued by a Court, or, in the absence of a Court issued-warrant, by a police officer in the course of investigation of offences.[148].

Similarly, Section 165 of the *Code of Criminal Procedure* permits for searches to be conducted by 'police officers in charge of police station or a police officer making an investigation' without first obtaining a warrant. Such a search may be conducted if he has 'reasonable grounds for believing that anything necessary for the purposes of an investigation into any offence which he is authorised to investigate may be found in anyplace within the limits of the police station of which he is in charge, or to which he is attached', and if, in his opinion, such thing 'cannotbe otherwise obtained without undue delay. Such officer must record in writing the grounds of his belief and specify 'so far as possible' the thing for which search is to be made[149].

However, in reality, these above mentioned necessities are more oftenly found breached or intruded. Courts have consistently held that not following these provisions would not make evidence obtained inadmissible, it would make the search irregular, not unlawful. Thus, in *State of Maharashtra* v. *Natwarlal Damodardas Soni*, where a

147 PrashantIyengar, *Limits to Privacy*, CIS/PRIVACY INDIA, http://ssm.com/ abstract=l807733 or http://dx.doi.org/10.2139/ssm.1807733 (April 12, 2011).

148 Basu, *supra* note 138.

149 The Code of Criminal Procedure, Sec. 165 (1973).

search was conducted under the *Customs Act* to recover smuggled gold, the Supreme Court held that: '*Assuming that the search was illegal it would not affect either the validity of the seizure and further investigation by the customs authorities or the validity of the trial which followed on the complaint of the Assistant Collector of Customs*'[150].

Furthermore, in a different case, *Radhakrishan* v. *State of U.P.* which involved an illegal search in contravention of the Code of Criminal Procedure, the Supreme Court held that:

> "So far as the alleged illegality of the search is concerned, it is sufficient to say that even assuming that the search was illegal the seizure of the Articles is not vitiated. It may be that where the provisions of Code of Criminal Procedure, are contravened the search could be resisted by the person whose premises are sought to be searched. It may also be that because of the illegality of the search the Court may be inclined to examine carefully the evidence regarding the seizure. But beyond these two consequences no further consequence ensues"[151].

India inherits the common law notion that 'a man's house is his castle' and also to the fouth amendment to the US Constitution which reads The right of the people to be secure in their person, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized[152] where the US Supreme Court had held unreasonable searches and seizures, without the issuance of a warrant on probable cause, to vitiate the principle of self-incrimination inherent in the Fifth Amendment of the US Constitution.[153]. But these claims are seem to be supercilious in light of the

---

150 Maharashtra v. NatwarlalDamodardasSoni, AIR 593 (SC 1980),1980 SCR (2) 340.

151 Radhakrishan v. State of U.P., Supp. 1 S.C.R. 408 (1963).

152 Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757 (1994).

153 Also, "Nor shall (any person) be compelled in any criminal case to be a witness against himself.". Refer: Boyd v. United States, 116 US 616 (1886) (considering the seizure of 35 cases of plate glass by the Collector); Weeks v. United States, 232 US 383 (1914) (considering the seizure of papers by the police, which showed the accused to have sent lottery tickets through the mail); Olmstead v. United States, 277 US 438 (1928) (Brandeis, J. dissenting that it would be a lesser evil for criminals to go free than for the Government to "play an ignoble part" by tapping phone conversations); Katz v. United States, 389 US 347 (1967) (finding that tapping into a telephone conversation would amount to a search and seizure and all the Fourth Amendment safeguards would apply); Terry v. Ohio, 392 US 1 (1968) (considering a confrontation on the street between a policeman and citizens to amount to a search and seizure);

cases discussed above. However, there is still hope. In a recent case, the Supreme Court struck down provisions of a legislation on grounds that it was too intrusive of citizens' right to privacy. The case involved an evaluation of the Andhra Pradesh Stamp Act which authorized the collector to delegate 'any person' to enter any premises in order to search for and impound any document that was found to be improperly stamped. Thus, for instance, banks could be compelled to cede all documents in their custody, including clients documents, for inspection on the mere chance that some of them may be improperly stamped. These banks were then compelled under law to pay the deficit stamp duty on the documents, even if they themselves were not party to the transactions recorded in the documents[154].

After an exhaustive analysis of privacy laws across the world, and in India, the Supreme Court held that in the absence of any safeguards as to probable or reasonable cause or reasonable basis, this provision was violative of the constitutionally guaranteed right to privacy 'both of the house and of the person'[155].And the given case has marked a high status for the protection of right to privacy in India.

4.3. Privacy of body and disclosure of intimate details

Privacy as a right is important but at the same time it cannot be the right which can hold back all the possible important information about one's self from all the different institutions which are in existence at all the conceivable periods.As in such a situation the very concept of societal coexistence wouldsolidifytrivial. This particular heading questions the entend of right to privacy in India context to one's own body where four major contentions has arisen before the Court of law, 1) the capacity orto what extend the state can order a person to undergo medical-examination, 2) to endure a assortment of "truth technologies" including narco analysis, brain mapping, etc., 3) questions relating to DNA testing and 4) to that of abortion. It will be seen later in most of the cases that the right to privacy being surrendered in the pretext of the other

---

Stanley v. Georgia, 394 US 557 (1969) (finding that the State had no business to tell a man what books to read in the privacy of his home). Refer also, Carol S. Steiker, "Second Thoughts About First Principles", 107 HARV. L. REV. (1994), p. 820 (justifying the principles of the Fourth Amendment on the grounds that 'individual liberties entail social costs').

154 Iyengar, *supra* note 148.

155 Distt. Registrar & Collector, Hyderabad v. Canara Bank, AIR 186 (SC 2005).

subjects and authorities gaing power over it having competing interest, which will be broadly discussed below.

4.3.1. Court-ordered Medical Examinations

Are the Courts empowered toobligea person to endure medical examinations against his/her will? The question leads to the evalution of the first judicial interpretation where in the case of *Sharda* v. *Dharmpat*, the Supreme Court held that they could. Here a man filed for divorce on that grounds that his wife suffered from a mental illness. In order to establish his case, he requested the Court to direct his wife to submit herself to a medical examination. The trial Court and the high Court both granted his application. On appeal to the Supreme Court, the woman contested the order on grounds firstly, that compelling a person to undergo a medical examination by an order of the Court would be violative of her right to 'personal liberty' guaranteed under Article 21 of the Constitution of India. Secondly, in absence of a specific empowering provision, a Court dealing with matrimonial cases cannot subject a party to undergo medical examination against his her volition. The Court could merely draw an adverse inference. The Supreme Court rejected these contentions holding that the right to privacy in Indiawas not absolute. If the 'respondent avoids such medical examination on the ground that it violates his/her right to privacy or for a matter right to personal liberty as enshrined under Article 21 of the Constitution of India, then it may in most of such cases become impossible to arrive at a conclusion. It may render the very grounds on which divorce is permissible nugatory.' The Court upheld the rights of matrimonial Courts to order a person to undergo medical test. Such an order, the Court held, would not be in violation of the right to personal liberty under Article 21 of the Constitution of India. However, this power could only be exercised if the applicant had a strong *prima facie case*, and there was sufficient material before the Court. Crucially, the Court held that if, despite the order of the Court, the respondent refused to submit herself to medical examination, the Court would be entitled to draw an adverse inference against him[156].

[156] Sharda v. Dharmpat, AIR 493 (4 SC 2003).

Thus it can be inferred from the aforesaid judgment that one's right to privacy over one's own body is not absolute where it comes to or in conflict to the statutory rights of the others. Therefore to say, a person is entitled to right to privacy of one's own body till the time that person is not grudging or depriving the statutory rights which was given by law to the other person, that is in the sense of above case the right to divorce.

4.3.2. Reproductive Rights

Another significant question relating to privacyof one's own body comes in the form of the extent to which a pregnant women can enjoy a right to privacy over her body and hence therefore making her own reproductive decisions. And the existence of any situations when the State can arbitrate and either order or forbid an abortion decision made by that of the reproductibe party. According to the *Medical Termination of Pregnancy Act* a pregnancy may be terminated before the twentieth week if:

(i) the continuance of the pregnancy would involve a risk to the life of the pregnant woman or of grave injury to her physical or mental health; or
(ii) there is a substantial risk that if the child were bom, it would suffer from such physical or mental abnormalities to be seriously handicapped.
(iii) where any pregnancy is alleged by the pregnant woman to have been caused by rape,
(iv) where any pregnancy occurs as a result of failure of any device or method used by any married woman or her husband for the purpose of limiting the number of children,

Consent for termination needs to be obtained from the guardian in cases of minors or women who are mentally ill. In all other cases, the woman herself must consent. Beyond the period of 20 weeks, the pregnancy may only be terminated if there is immediate danger to the life of the woman.[157]

[157] Medical Termination of Pregnancy Act, Sec. 3 (1971).

Under the given head, in August 2009, the Supreme Court heard an expedited appeal that was filed on behalf of a destitute mentally retarded woman who had become pregnant consequent to having been raped at a government run shelter. The government had approached the high Court seeking permission to terminate her pregnancy, which had been granted by that Court despite the finding by an 'expert body' of medical practitioners that she was keen on continuing the pregnancy. On appeal the Supreme Court held, very curiously, that the woman was not 'mentally ill', but 'mentally retarded', and consequently her consent was imperative under the Act.[158] However, not satisfied to stop there, the Court made several puzzling and contradictory observations. Firstly, the Court took the opportunity to affirm, generally, women's rights to make reproductive choices as a dimension of their 'personal liberty' as guaranteed by Article 21 (Right to Life and Personal Liberty) of the Constitution of India. The Court observed:

> "It is important to recognise that reproductive choices can be exercised to procreate as well as to abstain from procreating. The crucial consideration is that a woman's right to privacy, dignity and bodily integrity should be respected. This means that there should be no restriction whatsoever on the exercise of reproductive choices such as a woman's right to refuse participation in sexual activity or alternatively the insistence on use of contraceptive methods. Furthermore, women are also free to choose birth-control methods such as undergoing sterilisation procedures. Taken to their logical conclusion, reproductive rights include a woman's entitlement to carry a pregnancy to its lull term, to give birth and to subsequently raise children".[159]

However, the Court imitating the US judgment of *Roe* v. *Wade*[160]did affirmed that there was a compelling interest on the state to protect the life[161] of the forthcoming child though being in the mother's womb.

Secondly, the Supreme Court upheld the woman's consent as determinative and in doing so, categorically rejected the high Court approach. The Court held that since she suffered from 'mild mental retardation' this did not render her incapable of making

158 SuchitaSrivastava v. Chandigarh Administration, AIR 1 (9 SC 2009).

159 Iyengar, *supra* note 148, at 18.

160 *Supra* note 75.

161 Article 21 does not limit the abridgement of the right to life by the state to only cases where the state has compelling state interest. The Article reads "No person shall be deprived of his life or personal liberty except according to procedure established by law".

decisions for herself. Simultaneously, however, the Supreme Court proceeded gratuitously to apply the common law doctrine of *'parenspatriae'* to resume jurisdiction over the woman in her best interests. According to a Court-appointed expert committee, her mental age was close to that of a nine-year old child and she was capable of learning through rote memorisation and imitation and of performing basic bodily functions. In this light, the Court deemed in her 'best interests', as defined by an expert committee, to defer to her wishes. The findings recorded by the expert body indicate that her mental age is closet, that of a nine-year old child and that she is capable of learning through rote-memorisation and imitation. Even the preliminary medical opinion indicated that she had learnt to perform basic bodily functions and was capable of simple communications. In light of these findings, it is the best interests test alone which should govern the inquiry in the present case and not the substituted judgment test. If one disregards the liberalism of its outcome, there are various problems with this decision. Chiefly, the Supreme Court relied on the woman's expressed consent to deny the legitimacy of the high Court's decision in favour of abortion. Inexplicably, however, in the same move, the Supreme Court reserved to itself the right to adjudicate the 'best interests' of the woman. Thus, in relation to abortion, mentally retarded women are more autonomous than minor girls (since their own consent is determinative, rather than their guardians) but they are still less autonomous than 'normal' women (since their decisions are subject to adjudication based on what the Court thinks is in their best interests).[162]

4.3.3. DNA Tests in civil suits and its impact on the right to privacy

The Apex Court of India often left with the question to determine the privacy rights of one's own interior body, the blood, the tissue, the DNA, where there is by now, a strong line of cases decided by the Supreme Court in which our right to 'bodily integrity' has been held to not be absolute, and may be interfered with in order to settle many terrestrial issues. In most cases, this question has arisen in the context of the determination of paternity, either in divorce or maintenance proceedings. Central in the determination of these issues is Section 112 of the *IndianEvidence Act* which stipulates that birth of a child during the continuance of a valid marriage (or within 280days of its

[162] Iyengar, *supra* note 154, at 19.

dissolution) would be conclusive proof of legitimacy of that child, unless it can be shown that the parties to the marriage had no access to each other at any time when he could have been begotten[163].

It is evident from the provision discussed above the legal presumption which it has created for legitimacy that leaves hardly any room for futher logical discussion/ contention.Though many of the litigants have sought after for the acceptance of the medical evidence against the former legal presumption in the court of law, it is only in early 1990s when efforts have shown certain outcomes, where the legal precedents were set by taking medical evidence in cases which they measured as a fit one. But these kind of medical evidences often requires to go through various legal test, sometimes against one's own body, which has led to the initiation of the following era of judgments where the consideration is bestowed also upon the privacy rights of an individual along with the collection of the legal data of medical evidences.In one of the earliest and most frequently invoked cases, *Goutam Kundu* v.*State of West Bengal and Another* the Supreme Court laid down guidelines governing the power of Courts to order blood tests. The Court held:

> "1)Courts in India cannot order blood test as matter of course;
> 2)wherever applications are made for such prayers in order to have roving inquiry, the prayer for blood test cannot be entertained;
> 3)There must be a strong prima facie case in that the husband must establish on-access in order to dispel the presumption arising under section 112 of the *Evidence Act*;
> 4)The Court must carefully examine as to what would be the consequence of ordering the blood test; whether it will have the effect of branding a child as a bastard and the mother as an unchaste woman;
> 5)No one can be compelled to give sample of blood for analysis."[164]

It is to be noted that, on the particular facts of this case, the Supreme Court refused to order the respondent to submit to the test, since in its view, there was no prima facie case made out that cast doubts on the legal presumption of legitimacy. These guidelines have been frequently invoked in subsequent cases as the of in a complex set of facts, in *Ms. X*v. *Mr. Z and Another*, the Delhi High Court was called to consider whether a foetus had a 'right to privacy' or whether the mother of the foetus could assert a right to privacy on it's behalf. A woman had given birth to a still-born

---

163 Indian Evidence Act, Sec. 112 (1872).

164 GoutamKundu v. State of West Bengal and Another, AIR 2295 (SC 1993),1993 SCR (3) 917.

child and tissues from the foetus had been stored at the All India Institute of Medical Sciences. Her husband approached to obtain an order permitting a DNA test to be carried out to determine if he was the father. In her defence, the woman claimed that this would offend her right to privacy. The high Court reaffirmed the guidelines laid down in the *Gautam Kundu* case as discussed above, and also upheld the petitioner's right to privacy over her own body. However, the Court took the stance that she did not have a right of privacy over the foetus once it had been discharged from her body:

> The petitioner indeed has a right of privacy but is being not an absolute right, therefore, when a foetus has been preserved in All India Institute of Medical Science, the petitioner, who has already discharged the same cannot claim that it affects her right of privacy. However, if the petitioner was being compelled to subject herself to blood test or otherwise, she indeed could raise a defence that she cannot be compelled to be a witness against herself in a criminal case or compelled to give evidence against her own even in a civil case but the position herein is different. The petitioner is not being compelled to do any such act. Something that she herself has discharged, probably with her consent, is claimed to be subjected to DNA test. In that view of the matter, in the peculiar facts, it cannot be termed that the petitioner has any right of privacy.[165]

Henceforth, the decision has wide-ranging implications since it virtually divests control and ownership over any material that has been discarded from the body - from nails to hair to tissue samples.In a sense the *Ms. X* v. *Mr. Z* case arrives at identical conclusions without as much deliberation on its implications. It would be interesting to see how subsequent Courts interpret and apply this precedent. One of the most critical factors, consistently weighed by Courts alongside the privacy rights implicated, is the 'best interests' of the child[166]. Thus, in *Bhabani Prasad Jena* v. *Convenor Secretary, Orissa State Commission for Women & Another*, the Supreme Court quashed a high Court-mandated DNA test to determine the paternity of an unborn child in a woman's womb. In doing so, the Supreme Court observed:

> In a matter where paternity of a child is in issue before the Court, the use of DNA is an extremely delicate and sensitive aspect. One view is that when modem science gives means of ascertaining the paternity of a child, there should not be any hesitation to use those means whenever the occasion requires. The other view is that the Court must be reluctant in use of such

---

165 Ms. X v. Mr. Z and Another, AIR 217 (Delhi 2002).

166 *Id.*

> scientific advances and tools which result in invasion of right to privacy of an individual and may not only be prejudicial to the rights of the parties but may have devastating effect on the child. Sometimes the result of such scientific test may bastardise an innocent child even though his mother and her spouse were living together during the time of conception. In our view, when there is apparent conflict between the right to privacy of a person not to submit himself forcibly to medical examination and duty of the Court to reach the truth, the Court must exercise its discretion only after balancing the interests of the parties and on due consideration whether, for a just decision in the matter, DNA is eminently needed.[167]

With the instant case, a strong trend started conveying the interest of the child, when not declared as illegitimate and also that of the privacy rights of a mother. The both has created a amalgamated interest for one another, opposed to the interest of the father which are declared by the statutes, which the courts were unenthusiastic to decide or look upon for many years unless and untill they are compelled to do so. But does if effect the interests of a child when it is in conflict with the privacy rights of the respective parents, the question was well interpretated hereby. In a high profile case in 2010 of*Shri Rohit Shekhar* v. *Shri Narayan Dutt Tiwari*, the Delhi High was called upon to determine whether a man had a right to subject the person he named as his biological father to a DNA test. Contrary to the trend in the preceding cases, it was the biological father who pleaded his right to privacy in this case. The Court relied on international covenants to affirm the 'right of the child to know of her (or his) biological antecedents' irrespective of her (or his) legitimacy. The Court ruled:

> There is of course the vital interest of child to not be branded illegitimate; yet the conclusiveness of the presumption created by the law in this regard must not act detriment to the interests of the child. If the interests of the child are best sub- served by establishing paternity of someone who is not the husband of her (or his) mother, the Court should not shut that consideration altogether. The protective cocoon of legitimacy, in such case, should not entomb the child's aspiration to learn the truth of her or his paternity[168].

Over the time the Courts have tried to draw the dissimilarity between the concepts of legitimacy and paternity where the former draws its right from legal presumption and

---

167 Bhabani Prasad Jena v. Convenor Secretary, Orissa State Commission for Women & Another, AIR 2851 (SC 2010).

168 ShriRohitShekhar v. Shri Narayan DuttTiwari, 23 December, 2010, (June 25, 2009) http://indiankanoon.org/doc/504408/.

latter from reasonable and scientific legal evidences. But the Courts have made it very clear in almost all its judgments that the plaintiff is required to establish a *prima facie* case whereby it should ponder the contending interest of the privacy rights of those on which the test will be done and that of justice, before any order could be passed in favour of a DNA test. In this case, the petitioner was able to produce DNA evidence that excluded the possibility that his legal father was his biological father. In addition, photographic and testimonial evidence suggested that the respondent could be his biological father. On these grounds the Delhi High Court ordered the respondent to undergo a DNA test. This was upheld in an appeal to the Supreme Court[169]. Henceforth, from the abovementioned judgments, it specifically bring out the idea that the 'best interest of a child' is what which is considered before touching the privacy rights of the either of the parents of the child on which the interest is been bestowed upon. That is to say, if the two of them are if ever in conflict, then it is the former which shall customarily prevail over the other.

4.3.4. Bodily Effects and the right to privacy

Under the given head, the bodily effects that are considered are consisting of the fingerprints, handwriting samples, photographs, Irises, Narco-analysis, brain maps, DNA and many such others. It is to be noted that the human body easily betrays itself. We are incessantly dropping residues of our existence wherever we go, from shedding hair and fingernails, to fingerprints and footprints, handwriting which, through use of modem technology, can implicate our bodies, and identify us against our will. Not even our thoughts are immune as new technologies like brain mapping pretend to be able to harvest psychic clues from our physiology. In this section we explore occasions when the state may compel us to 'perform' our existence for instance, by submitting to photography, providing finger impressions or handwriting samples, submit to narco-analysis and truth tests, and more recently to provide iris scan data or our DNA[170].

Section 73 of the *Indian Evidence Act* stipulates that the Courtmay direct any person present in the Court to write any words or figures for the purpose of enabling the

169 *Id.*

170 Iyengar, *supra* note 148, at 24.

Court to compare the words or figures so written with any words or figures alleged to have been written by such person.[171]The above stated provision was duly construedby the Apex Court of the country in the judgment of *State of U.P.* v. *Ram Babu Misra*, where it was held that there must be 'some proceeding before the Court in which it might be necessary to compare such writings'. This specifically excludes, say, a situation where the case is still under investigation and there is no present proceeding before the Court. 'The language of provision of Section 73 does not permit a Court to give a direction to the accused to give specimen writings for anticipated necessity for comparison in a proceeding which may later be instituted in the Court.[172]

In addition to the above, the *Code of Criminal Procedure* was amended in 2005 to make a valid entry of the collection of the numerous number of medical details when the accused is arrested, leaving the decisive factor in the hands of the judiciary whether such collection of information will lead to violation or intrusion in the right to privacy of a person. Section 53of the *Code of Criminal Procedure* provides that upon arrest, an accused person may be subjected to a medical examination if there are 'reasonable grounds for believing' that such examination will afford evidence as to the crime. The scope of this examination was expanded in 2005 to include 'the examination of blood, blood-stains, semen, swabs in case of sexual offences, sputum and sweat, hair samples and finger nail clippings by the use of modem and scientific techniques including DNA profiling and such other tests which the registered medical practitioner thinks necessary in a particular case.[173]

In one of the recent cases the Orissa High Court affirmed the legality of ordering a DNA test in criminal cases to ascertain the involvement of persons accused. Refusal to co-operate would result in an adverse inference drawn against the accused. After weighing the privacy concerns involved, the Court laid down the following considerations as relevant before the DNA test could be ordered:

(i) the extent to which the accused may have participated in the commission of the crime;

---

171 Indian Evidence Act, Sec. 73 (1872).

172 State of U.P. v. Ram BabuMisra, AIR 791 (SC 1980), 1980 SCR (2)1067, (1980) 2 SCC 343.

173 Code of Criminal Procedure, Sec. 53 (1973).

(ii) the gravity of the offence and the circumstances in which it is committed;
(iii) age, physical and mental health of the accused to the extent they are known;
(iv) whether there is less intrusive and practical way of collecting evidence tending to confirm or disprove the involvement of the accused in the crime;
(v) the reasons, if any, for the accused for refusing consent.[174]

Most recently the draft DNA Profiling Bill pending before the Parliament attempts to create an ambitious centralized DNA bank that would store DNA records of virtually anyone who comes within any proximity to the criminal justice system. Specifically, records are maintained of suspects, offenders, missing persons and 'volunteers'. The schedule to the Bill contains an expansive list of both civil and criminal cases where DNA data will be collected including cases of abortion, paternity suits and organ transplant. Provisions exist in the bill that limit access to and use of information contained in the records, and provide for their deletion on acquittal. These are welcome minimal guarantors of privacy[175].

It is evident that the utility of this mass of information like that of fingerprints, handwriting samples and photographs, DNA data, etc., in solving crimes is immense. Without saying a word, it is possible for a person to be convicted based on these various bodily affects, the human body constantly bears witness and self-ineriminates itself. Both handwriting and finger impressions beg the question of whether these would offend the protection against self-incrimination contained in Article 20(3)[176] of Indian Constitution which provides that 'No person accused of any offence shall be compelled to be a witness against himself.'[177] This argument was considered by the Supreme Court in the *State of Bombay* v. *Kathi Kalu Oghad and others* where the petitioner contended that the obtaining of evidence through legislations such as the *Identification of Prisoners Act* amounted to compelling the person accused of an offence 'to be a witness against himself' in contravention of Article 20(3) of the Constitution. The Court held that there was no infringement of Article 20(3) of the Constitution in compelling an accused person to give his specimen handwriting or signature, or impressions of his

174 Thogorani Alias K. Damayantivs v. State of Orissa and Ors., 2004 Cri L J 4003 (Ori).
175 Iyengar, *supra* note, at 19.
176 INDIAN CONST. art. XX, clause 3.
177 *Id.*

thumb, fingers, palm or foot to the investigating officer or under orders of a Court for the purposes of comparison. Compulsion was not inherent in the receipt of information from an accused person in the custody of a police officer; it will be a question of fact in each case to be determined by the Court on the evidence before it whether compulsion had been used in obtaining the information.[178]

Over the past two decades, forensics has shifted from trying to track down a criminal by following the trail left by her bodily traces, to attempting to apply a host of invasive technologies upon suspects in an attempt to escape truth and lies directly from their body. One statement by Dr M.S. Rao, Chief Forensic Scientist, Government of India captures this shift:

> Forensic psychology plays a vital role in detecting terrorist cases. Narco-analysis and brainwave fingerprinting can reveal future plans of terrorists and can be deciphered to prevent terror activities. Preventive forensics will play a key role in countering terror acts. Forensic potentials must be harnessed to detect and nullify their plans. Traditional methods have proved to be a failure to handle them. Forensic facilities should be brought to the doorstep of the common man. Forensic activism is the solution for better crime management.[179]

Although there are several such 'technologies' which operate on principles ranging from changes in respiration, to mapping the electrical activity in different areas of the brain, what is common to them all, in Lawrence Liang's words is that they 'maintain that there is a connection between body and mind; that physiological changes are indicative of mental states and emotions; and that information about an individual's subjectivity and identity can be derived from these physiological and physiological measures of deception.'[180]

Hence, further contentions arises on the legality of the above mentioned techniques against the constitutional protection of the concept of self-incrimination and that of intruding the privacy rights of others. In a case in 2004 the Bombay High Court upheld these technologies by applying the logic of the *Kathi Kalu Oghad* case discussed above. The Court drew a distinction between 'statements' and 'testimonies' and held

---

178 State of Bombay v. KathiKaluOghad and Ors., AIR 1808 (SC 1961).

179 Sarai Reader 07: Frontiers, and nothing but the truth, so help me science, DELHI: CSDS, Delhi, 100-110, (June 20, 2018), http://www.sarai.net/publications/readers/07-frontiers/100-10_lawrence.pdf.

180 *Id.*

that what was prohibited under Article 20(3) were only ‘statements’ that were made under compulsion by an accused. In the Court’s opinion, ‘the tests of Brain Mapping and Lie Detector, in which the map of the brain is the result, or polygraph, then either cannot be said to be a statement”. At the most, the Court held, it can be called the information receivedor taken out from the witness.[181]

This position was however overturned recently by the Supreme Courtdecision in the case of *Selvi v. State of Karnataka*. In contrast with the Bombay High Court, the Supreme Court expressly invoked the right of privacy to hold these technologies unconstitutional.

> Even though these are non- invasive techniques the concern is not so much with the manner in which they are conducted but the consequences for the individuals who undergo the same. The use of techniques such as ‘Brain Fingerprinting’ and ‘FMRI-based Lie-Detection’ raise numerous concerns such as those of protecting mental privacy and the harms that may arise from inferences made about the subject's truthfulness or familiarity with the facts of a crime.[182]

Further down, the Court held that such techniques invaded the accused’s mental privacy which was an integral aspect of their personal liberty.

> There are several ways in which the involuntary administration of either of the impugned tests could be viewed as a restraint on ‘personal liberty’. The drug induced revelations or the substantive inferences drawn from the measurement of the subject's physiological responses can be described as an intrusion into the subject's mental privacy.[183]

Hereby after referring the issue, the Supreme Court absorbed that no individual should be forcibly subjected to any of the techniques in question, whether in the context of investigation in criminal cases or otherwise. Doing so would amount to an unwarranted intrusion into personal liberty, which will finally lead to the violation of one’s right to privacy. The Court however, left open the option of voluntary submission to such techniques and endorsed the following guidelines framed by the *National Human Rights Commission*:

---

181 Ramchandra Ram Reddy v. State of Maharashtra, 1 (2205) CCR 355 (DB).
182 Selvi v. State of Karnataka, SCC 263 (7 SC 2010).
183 *Id.*

(i) No Lie Detector Tests should be administered except on the basis of consent of the accused. An option should be given to the accused whether he wishes to avail such test.

(ii) If the accused volunteers for a Lie Detector Test, he should be given access to a lawyer and the physical, emotional and legal implication of such a test should be explained to him by the police and his lawyer.

(iii) The consent should be recorded before a judicial magistrate.

(iv) During the hearing before the magistrate, the person alleged to have agreed should be duly represented by a lawyer.

(v) At the hearing, the person in question should also be told in clear terms that the statement that is made shall not be a 'confessional' statement to the magistrate but will have the status of a statement made to the police.

(vi) The magistrate shall consider all factors relating to the detention including the length of detention and the nature of the interrogation.

(vii) The actual recording of the lie detector test shall be done by an independent agency (such as a hospital) and conducted in the presence of a lawyer.

(viii) A full medical and factual narration of the manner of the information received must be taken on record.

Although the right against self-incrimination and the inherent fallaciousness of the technologies were the main ground on which decision ultimately rested, this case is valuable for the Court's articulation of a right of 'mental privacy' grounded on the fundamental right to life and personal liberty.[184]

4.4. Privacy of Records

It can be stated that since at least the mid-nineteenth century, we have been living in what *Nicholas Dirks* has termed an 'ethnographic state', engaged relentlessly and fetishistically in the production and accumulation of facts about us. From records of birth and death, to our academic records, most of our important transactions, our income tax filings, our food entitlements and our citizenship, most of us have assuredly been documented and lead a shadow existence somewhere on the files. Not only does

[184] Iyengar, *supra* note, at 27.

the government keep records about us, but a host of private service providers including banks, hospitals, insurance and telecommunications companies maintain volumes of records about us. In this section of dissertation, it looks at the privacy expectation of records both maintained by the government and the private sector.Various statutes require records to be maintained of activities conducted under their authority and entire bureaucracies exist solely in service of these documents. Thus, for instance, the Registration Act requires various registers to be kept which record documents which have been registered under the Act. Once registered under this Act, all documents become public documents and State Rules typically contain provisions enabling the public to obtain copies of all documents for a fee. Similarly, a number of legislation, typically dealing with land records at the state level contains enabling provisions that allow the public to access them upon payment of a fee[185].

And when, where no provisions are provided within the statute itself that enable the public to obtain records, two recourses are still available. Firstly, the *Evidence Act* enables courts to access records maintained by any government body. Secondly, private citizens may access records kept in public offices through the *Right to Information Act*. Each of these avenues is described in some details below[186]. Section 74 of the *Evidence Act* defines 'public documents' as including the following:

1. *Documents forming the acts, or records of the acts*

   (i)Of the sovereign authority,
   (ii)Of Official bodies and the Tribunals, and
   (iii)Of public officers, legislative, judicial and executive, of any part of India or of the Commonwealth, or of a foreign country.

2. *Public records kept in any state of private documents[187].*

It is clear from this definition that most records maintained by any government body are regarded as public documents. Section 76 mandates that every public officer 'having custody of a public document, which any person has a right to inspect, shall give that person on demand a copy of it on payment of the legal fees there for together

185 GautamSwarup, *Why Indian Judges would Rather be Originalist: Debunking Practices of Comparative Constitutional Law in India*, 5 INDIAN JOURNAL OF CONSTITUTIONAL LAW 62, 55-74 (2011).
186 *Id.*
187 Indian Evidence Act, Sec. 74 (1872).

with a certificate written at the foot of such copy that it is a true copy of such document or part thereof.'[188]

In addition to the *Evidence Act*, copies of documents may also be obtained under the *Right to Information Act*, 2005 which confers on citizens the right to inspect and take copies of any information held by or under the control of any public authority. Information is defined widely to include 'any material in any form, including records, documents, memos, e-mails, opinions, advices, press releases, circulars, orders, logbooks, contracts, reports, papers, samples, models, data material held in any electronic form and information relating to any private body which can be accessed by a public authority under any other law for the time being in force'.Section 8(1)(j) of the Act exempts 'disclosure of personal information the disclosure of which has no relationship to any public activity or interest, or which would cause unwarranted invasion of the privacy of the individual' unless the relevant authority 'is satisfied that the larger public interest justifies the disclosure of such information.'[189]But this impose a serious issue on the privacy rights of a person without whose consent or knowledge such information was retrived by the respective authority. The question of the satisfaction of the relevant authorities to intrude one's personal information is also upon the judicious decision of the judiciary where no specific positive privacy law is there, whereby the same could be referred by the victim of whose privacy rights is violated in the court of law.

In an remarkable case of *Mr. Ansari Masud A.K* v. *Ministry of External Affairs*, the Central Information Commission has held that 'details of a passport are readily made available by any individual in a number of instances, example to travel agents, at airline counters, and whenever proof of residence for telephone connections etc. is required. For this reason, disclosure of details of a passport cannot be considered as causing unwarranted invasion of the privacy of an individual and, therefore, is not exempted from disclosure under Section 8(l)(j) of the RTI Act.' This is despite the fact that nothing in the Passport Act itself authorizes disclosure of any documents under any

188 Indian Evidence Act, Sec. 76 (1872).
189 Right to Information Act, Sec. 8(1)(j) (2005).

circumstances.[190] However, the *Right to Information Act* isn't as convenient a vehicle for privacy abuse as this case may suggest. The RTI adjudicatory apparatus has on several occasions upheld the denial of information on grounds of privacy violation, most famously in a case where an applicant sought information from the Census Department on the 'religion and faith' of Sonia Gandhi, the President of the largest party currently in power in India. Both the Central Information Commission, the apex body adjudicating RTI appeals as well as the Punjab and Haryana High Court upheld the denial of information as it would otherwise lead to an unwarranted incursion into her privacy.[191]

A similar concept of 'public interest' would seem to apply when private companies disclose personal information without a person's consent. Without delving into the issue in too much detail, it would suffice here to mention one of the most important cases to have come up on the issue. In *Mr. X* v. *Hospital Z*, a person sued a hospital for having disclosed his HIV status to his fiance without his knowledge resulting in their wedding being called off. The Supreme Court held that the hospital was not guilty of a violation of privacy since the disclosure was made to protect the public interest. While affirming the duty of confidentiality owed to patients, the court ruled that the right to privacy was not absolute and was subject to such action as may be lawfully taken for the prevention of crime or disorder or protection of health or morals or protection of rights and freedom of others.[192]

4.5. Conclusion

To conclude it can be stated that right to privacy is chieflya very new phenomenon where it is still in its developing nature. But the major problem with it is that the law on privacy has not kept pace with technological development. Even today, in no country does the right to privacy enjoy the status of a specific constitutional right where privacy law has evolved largely through judicial pronouncements. Some of the countries have been successful in enacting a specific positive laws for the protection

---

190 CIC/OK/A/2008/987/AD, December 22, 2008 (June 22, 2018), http://indiankanoon.org/doc/1479476/.

191 Anon, *2010 High Court dismisses appeal seeking information on Sonia Gandhi's religion*, NDTV ONLINE, (June 21, 2018), http://www.ndtv.com/article/india/high-court-dismisses-appeal-seeking-informationon-sonia-gandhi-s-religion-69356.

192 Mr. X v. Hospital Z, SCC 500 (1 SC 2003), p.40.

and promotion of the privacy rights, unlike that of India where the decision of one's privacy right is violated or not are still bestowed on the hand of the judiciary, which they do by interpreting the provisions of the Constitution or that of other provisions of laws relating to privacy, as has been discussed above. But what today is required with the swelling technological changes and in a techno-friendly era where the violation of such rights are more prominent, an absolute positive law to protect the privacy rights of the people of India directly in any form of violation, without being waiting for the decision of the judiciary to come and pursue whether such a violation is even a violation of privacy rights or not.

CHAPTER 5

RIGHT TO PRIVACY: RECENT TRENDS IN INDIA

Right to privacy as a concept is fundamentallya freshlyestablished phenomenon. In fact it can be said it is still developing. Now right to privacy is passing through a most crucial era that is the era of information and technology and hence it is one of the prominent issue to study how such trends in the recent developments have effected and prompted the cherished right of right to privacy in relation to India.

5.1. Modern media and technology and privacy rights in India

The development of the media in modern times has a special relevance to the evolution of the law of privacy. The media has made it possible to bring the private life of an individual into the public domain, thus exposing him to the risk of an invasion of his space and his privacy. At a time when information was not so easily accessible to the public, the risk of such an invasion was relatively remote. In India, newspapers were, for many years, the primary source of information to the public. Even they had a relatively limited impact, given that the vast majority of our population was illiterate. This has changed with a growth in public consciousness, a rise in literacy and perhaps most importantly, an explosion of visual and electronic media which have facilitated an unprecedented information revolution.[193]Though at many times, it has worked as an asset for uplifting the essence of the privacy rights in India, in today's modern era it often come across as the intruder of the very right which it has helped to develop.

The notion of fundamental rights, such as a right to privacy as part of right to life, is not merely that the State is enjoined from derogating from them. It also includes the responsibility of the State to uphold them against the actions of others in the society, even in the context of exercise of fundamental rights by those others. The right to privacy in India has failed to acquire the status of an absolute right. The right in comparison to other competing rights, like, the right to freedom of speech & expression, the right of the State to impose restrictions on account of safety and security of the

193 Utkarsh Amar, *Right to Privacy in the Dawn of Information and Communication Technology- A Critical Review*, 3 INTERNATIONAL JOURNAL OF LAW AND LEGAL JURISPRUDENCE STUDIES 290, 287-296 (2012).

State, and the right to information, is easily relinquished. The exceptions to the right to privacy, such as, overriding public interest, safety and security of the State, apply in most countries. Nonetheless, as the paper demonstrates, unwarranted invasion of privacy by the media is widespread. The Indian norms or code of ethics in journalism fail to make such a distinction between public and private space. The Indian media violates privacy in day-to-day reporting, like overlooking the issue of privacy to satisfy morbid curiosity. Nor do the guidelines impose any restrictions on photographing an individual without seeking express consent of the individual.[194]

For instance, under the media venture itself, television channels have started a series of investigative attempts with hidden cameras and other espionage devices in the form of sting operations. The advent of miniaturized audio and video technology, specially the pinhole camera technology, enables one to clandestinely make a video/audio recording of a conversation and actions of the oether individuals. In law enforcement, a sting operation is an operation designed to catch a person committing a crime by means of deception. A typical sting will have a law-enforcement officer or cooperative member of the public play a role as criminal partner or potential victim and go along with a suspect's actions to gather evidence of the suspect's wrongdoing. Now the moot question that arises is whether it is for the media to act as the law enforcement agency?[195]

It is important to point out here that the carrying out of a sting operation may be an expression of the right to free press but it caries with it an indomitable duty to respect the privacy of others. The individual who is the subject of a press or television item has his or her personality, reputation or career dashed to the ground after the media exposure. He too has a fundamental right to live with dignity and respect and a right to privacy guaranteed to him under Article 21 of the Constitution of India[196], as interpreted by the Indian judiciary respectively.

Further, advances in computer technology and telecommunications have dramatically increased the amount of information that can be stored, retrieved, accessed

194 Uppaluri, *supra* note 7.

195 RICHARD A. GLENN, THE RIGHT TO PRIVACY: RIGHTS AND LIBERTIES UNDER THE LAW 7-10 (ABC-CLIO, Inc., 2003).

196 *Id.*

and collated almost instantaneously. An enormous amount of personal information is held by various bodies, both public and private, the police, the income tax department, banks, insurance agencies, credit-rating agencies, stockbrokers, employers, doctors, lawyers, marriage bureaus, detectives, airlines, hotels and so on. Till recently, this information was held on paper; the sheer Vol. and a lack of centralization made it hard to collate with the result that it was very difficult for one body or person to use this information effectively. In the Internet age, information is so centralized and so easily accessible that one tap on a button could throw up startling amounts of information about an individual. This enables public authorities to keep a closer watch over the individual.[197]

It is to be noted that, it doesn't end with public authorities. There are other Big Brothers watching everywhere. Every time you log on to the Internet you leave behind an electronic trail. Websites and advertising companies are able to track users as they travel on the Internet to assess their personal preferences, habits and lifestyles. This information is used for direct marketing campaigns that target the individual customer. Every time you use your credit card you leave behind a trail of where you shopped and when, what you bought, your brand preferences, your favorite restaurant. Further, employee privacy is under siege, employers routinely use software to access their employees' email and every move of the employee. Furthermore, field sales representatives have their movements tracked by the use of location-based tracking systems in new wireless phones.Technology blurs the traditional boundaries between systems. Techniques such as data mining ensure that every bit of valuable information is extracted and logged. Data matching enables linkages to be made between the contents of previously uncorrelated databanks. The move towards convergence will further blur traditional distinctions between activities, technologies and regulatory schemes. Information obtained by private agencies is used (and misused) not only by the private sector but is easily accessed by public authorities. Police and tax authorities the world over are known to rely on the private sector for information about suspects and tax evaders. Seemingly innocuous information disclosed in a specific limited

[197] Amar, *supra* note 194,at 292.

environment may be collated and used in a completely unforeseen and startling context.[198]

Moreover, the law on privacy has not kept pace with technological development. Even today, in no country does the right to privacy enjoy the status of a specific constitutional right. Privacy law has evolved largely through judicial pronouncement. As technology has advanced, the way in which privacy is protected and violated has changed with it. In the case of some technologies, such as the printing press or the Internet, the increased ability to share information can lead to new ways in which privacy can be breached.[199]As written by law professor and author Jeffrey Rosen, the Internet has brought new concerns about privacy in an age where computers can permanently store records of everything, where every online photo, status update, Twitter post and blog entry by and about us can be stored forever. Hence the possibility and ability to do online inquiries about individuals has also expanded dramatically over the last decade. According to some experts, many commonly used communication devices may be mapping every move of their users. Senator Al Franken has noted the seriousness of iPhones and iPads having the ability to record and store users locations in unencrypted files, although Apple denied doing so.[200]

Today in the blink of an eye any information can be gathered by both the private as well as public enterprises. Modern media, technological advancements and high communication skills have made it possible to make this world a global hut where one's information, whether public or private, is easily accessible by any other organisation for its own purposes, sometimes initiating the gross violation of the privacy rights by its acts. But these advancements have evolved privacy and one's data protection as one of the biggest problems in this new electronic era. At the heart of the Internet culture is a force that wants to find out everything about you. And once it has found out everything about you and two hundred million others, that's a very valuable asset, and people will be tempted to trade and do commerce with that asset. This wasn't the information that people were thinking of when they called this the information age, which violates its very right to privacy itself.It can be said that the current focus on the right to privacy is

198 *Id.*

199 Iyengar, s*upra* note 148.

200 A.S. Popkin Helen, *Govt. officials want answers to secret iPhone tracking*, MSNBC TECHNOLOGY (2011).

based on the realities of the digital age. India is rapidly becoming a digital economy and problems like ID theft, fraud and misrepresentation are real concerns. Persons information is out there, but the existence of such technological advancements have made many use such advances and development in a dire action, using the person's information in a wrongful manner for one's own gain. These has also led to question the Aadhaar law which was enacted in India, it being coming in clash with the privacy rights of others. And only because of such magnitudes, there is a great requirement of the data protection laws which has emerged in India considering the international instruments and also the legislations of other nations.

5.2. AADHAAR and Right to Privacy

Another recent trend in India which is leaving its mark is the evolution of the concept of AADHAAR and the violation and protection of privacy rights by the use of new technological advancements under the scheme. Indian polity has been continuously debating on merits and demerits of clouding data of one and all citizens of the country through a 12-digit Unique Identity Number (hereinafter referred as UID) system ever since the concept of AADHAAR has been introduced. This UID system carry necessary biometric data, which if falls in the wrong hands can be very dangerous to the society. Aadhaar is a huge database of biometric and different points of interest of a great many individuals; the issue that needs consideration is, since holders of information should be legitimately in charge of the information that they gather and hang for the information suppliers.The absence of a proper enacted law for the protection of data, authoritative investigation and in this manner administrative authorization for this anticipates is alarming. Even after the enactment of the legislation, there are no legitimate commitments on the Unique Identification Authority of India on the utilization of this information, either as far as its trustworthiness or for ensuring the national separating with touchy information.[201]

[201] SuhrithParthasarathy, *Privacy, Aadhaar and Constitution*, THE HINDU CENTRE FOR POLITICS AND PUBLIC POLICY 5, 1-6 (2017).

5.2.1. Nilekani's Idea of UID

The basic concept of having an identity in numerous nations is taken for granted. India tried to attain an advanced and standard identification system for the population since India was lacking a dominant identification system and came out with the idea of Aadhaar to identify each and every individual of the nation. Aadhaar was developed with the objective to tackle the problem of significant problem of introducing the more residents of India into the formal economy, provide greater access to the benefits and preventing country from the embarrassing situation of corruption and malfeasance. After great deal of efforts and consideration, Nilekani and his team proposed a system where the biometric technology would play the leading role to make sure that, the uniqueness of the identity and prevent the fraud. The proposed technological and institutional infrastructure of Aadhaar was set too high that, it had to be able to eliminate any kind of duplication and faking of identities which were well known in the current and prevalent system in the country.[202]

The concept of Aadhaar is defined as "*Aadhaar would also be a foundation for the effective enforcement of individual rights. A clear registration and recognition of the individual's identity with the state is necessary to implement their rights –to employment, education, food, etc. The number, by ensuring such registration and recognition of individuals, would help the state deliver these rights*."[203] Hence, the government through the notification dated 28 January 2009 established an institution named Unique Identification Authority of India which was assigned with the task to link each and every single person of the country system by allotting them a unique identity number. Aadhaar project led to the establishment of one of world's largest biometric data system.[204] Aadhaar soon after its introduction became the leading biometric data system of world as they lead the database of Federal Bureau of Investigation with a huge margin as per the reports released. Behind the introduction Biometric identity system, the basic idea was clearly mentioned in the notification dated 28 January 2009, but the authority setup through that notification had a great question

202 *Id.*

203 *Concept*, Unique Identification Authority of India, http://uidai.gov.in/uid-brand/concept.html (last updated June 10, 2016).

204 Unique Identification Authority of India, http://www.uidai.gov.in/images/notification28jan2009.pdf (last updated June 10, 2016).

to answer, and that too regarding legality of the Aadhaar, as it was conflicting with the very right of privacy which was well established within the defination of fundamental right of Article 21 in the Constitution of India.[205]

5.2.2. Legal issues with the Aadhaar

The big and the basic question which can be put forward with regard to UIDAI is that, how a authority can established without any legislative baking of it. The *Aadhaar (Targeted Deliveryof Financial and Other Subsidies, Benefits and Services) Act*, 2016 was enacted and notified on 26th March 2016, which was introduced in the parliament as money bill[206]. The object of the Act was to provide, as good governance, efficient, transparent, and targeted delivery of subsidies, benefits and services, the expenditure for which is incurred from the Consolidated Fund of India, to individuals residing in India through assigning of unique identity numbers to such individuals and for matters connected with it.[207]

Legal existence of the authority was challenged in the case of *Justice K.S Puttaswamy (Retd.)* v. *Union of India*, through a PIL where, it was contended by the Petitioners that, there are no safeguards or penalties and no legislative backing for obtaining personal information and if any violation of the privacy rights been done, and the proposed law introduced by the government has been rejected by the Parliamentary Standing Committee on Finance.[208]Provisions for collection and retention of biometric data have been held impermissible in the United Kingdom and France by their top courts on the basis of violation of the privacy rights of the people. It was also contended before the Hon'ble Supreme Court that, 'the scheme is unconstitutional as applicants are required to part with personal information on biometrics, iris and fingerprints, infringing their right to privacy, which is held part of the fundamental right to life under

---

205 *Id.*

206 K. R Srivats, *Aadhaar legislation tabled as a money Bill*, THE HINDU (June 15, 2018), http://www.thehindubusinessline.com/economy/new-aadhaar-bill-introduced-as-money-bill-in-lok-sabha/article8309587.ece.

207 SatyaVratYadav and Vasundhara Anil Kaul, *Right to Privacy: Redefining Social Security in India*, 3 INTERNATIONAL JOURNAL OF LAW AND LEGAL JURISPRUDENCE STUDIES 489, 482-496 (2012).

208 Justice K.S Puttaswamy (Retd.) v. Union of India, Writ Petition(s) (Civil) No(s). 494/2012.

Article 21 of the Constitution'[209] and also have the tendency of privacy violation by governmental and non-government enterprises by using such information about a person in a negative manner for its own unnatural benefits to be fulfilled.

Afterwards it was claimed by the Attorney General that, the invasion of privacy is of no consequence because privacy is not a fundamental right and has no meaning under Article 21. The right to privacy is not a guaranteed under the Constitution, because privacy is not a fundamental right. To the above mentioned contentions of the parities, court replied that, the invasion of privacy is of no consequence because privacy is not a fundamental right and has no meaning under Article 21. The right to privacy is not a guaranteed under the Constitution, because privacy is not a fundamental right. Privacy telescopes to liberty and the breach of privacy leads to a violation of liberty which is protected under Article 21 of the Constitution.[210]

Also it was contented by the petitioners that, in this case of data collection ultimate ownership of the data is held by UIDAI and hence they can use it for commercial purpose as well. To thiscontention, court replied held that, no data shared with UIDAI can be shared with anyone else without consent of the person whose data is to be shared. Court also held that, in case where there is a criminal investigation is pending; sharing of data by UIDAI depends on the order of the court.[211]But this cannot serve as a solution, as there are further challenges which are associated with the right to privacy and the scheme of Aadhaar.

There has been one more instance where the case of sharing of data by UIDAI, where the controversy was brought in the notice of the Superior Court of the country after UIDAI was aggrieved by the order of Bombay High Court. In this case, a girl aged seven years was gangraped. To crack the investigation, it was court ordered UIDAI to provide the database of all enrolled people to CBI, so that they can check the fingerprints found on the crime scene with the database. Aggrieved by the order of Court, authority approached Bombay High Court, and contended that database is for

---

209 J. Venkatesan, *Don't tie up benefits to Aadhaar: Court tells Centre*, THE HINDU (June 15, 2018) http://www.thehindu.com/todayspaper/tp-national/dont-tie-up-benefits-to-aadhaar-court-tellscentre/ article5162 837.ece.

210 *Supra* note 215.

211 *Id.*

civilians use and not to be used as forensic database. But Hon'ble Court recorded that, the UIDAI had agreed to test the competence of its database in comparing the chance fingerprints with its biometric record and also asked the director general of the Central Forensic Science Laboratory to examine the technological capabilities of the UIDAI database. This case was later on clubbed with the PIL filled by *Justice K.S Puttaswamy (Retd.)* v. *Union of India* and was argued on the ground of Right to Privacy[212].

5.2.3. Aadhaar and its challenges

There are many issues which are haunting the issue of privacy all the time after introduction of UIDAI where at the basic contention comes with the issue that UIDAI while enrolling and collecting the biometric data from the people uses many private parties for the respective work. There can be no guarantee that the some of the collected biometric data will not remain in private hands, leading to the possibility of misuse, through the modern media and technological advancements as has been discussed above, grossly violating the privacy rights of the person as a whole.

Furthermore, Aadhaar is under the scanner of Supreme Court because; it has been claimed by various that it Aadhaar will violate right to privacy of the people enrolled herein. Some of the complications of the Act are discussed hereunder:

- Act is silent regarding consent being acquired in case of the enrolling agency or registrars. However, Section 8 provides that any requesting entity will take consent from the individual before collecting his/her Aadhaar information for authentication purposes, though it does not specify the nature.
- Section 3 of the Act states that at the time of enrolment and collection of information, the enrolling agency shall notify the individual as to how their information will be used; what type of entities the information will be shared with; and that they have a right to see their information and also tell them how they can see their information. However, the Act is silent regarding notice of name and address of the agency collecting and retaining the information. Moreover, there is no guarantee that becuase notification has been provided to

[212] Unique Identification Authority of India & another v. Central Bureau of Investigation, Special Leave to Appeal, (Crl.) No(s).2524/2014.

the individual, the information of the individual will not be used for in a wrongful manner or will be misused by various governmental and non governmental organisations for its own unjust enrichment.

- The Aadhaar Act does not provide an opt- out provision and also does not provide an option to withdraw consent at any point of time. Section 7 of the Aadhaar Act actually implies that once the Central or State government makes Aadhaar authentication mandatory for receiving a benefit then the individual has no other option but to apply for an Aadhaar number. The only concession that is made is that if an Aadhaar number is not assigned to an individual then s/he would be offered some alternative viable means of identification for receiving the benefit. Government is very rashly moving to that step when they will declare Aadhaar mandatory to avail benefits of social security scheme. However this step of central government timely went in under the scanner of Supreme Court.
- Section 28 of the Act states that the UIDAI must ensure the security and confidentiality of identity information and authentication records. It also states that the Authority shall adopt and implement appropriate technical and organizational security measures, and ensure the same are imposed through agreements/arrangements with its agents, consultants, advisors or other persons. However, it does not mention which standards/measures have to be adopted by all the actors in Aadhaar ecosystem for ensuring the security of information, though it can be argued that if the contractors employed by the UIDAI are body corporate then the standards prescribed under the IT Rules would be applicable to them.[213]

India is one of the first countries in the world that has initiated a biometric identification system for all residents. This new Act of 2016 intends to connect all the financial and subsidized benefits as well as the banking to the Aadhaar number. Identity theft may not be possible from biometric data but, collection of data is done by the hired private entities and there is nothing in this act to deal with the issue of misuse of data collected thereto. Also UIDAI, data repository has to be very cautious from the

[213] Praveen Kumar and Chander Kant, *Unique Identification System in India: A Big Challenge*, 5 INTERNATIONAL JOURNAL OF INFORMATION TECHNOLOGY AND KNOWLEDGE MANAGEMENT 450, 447-451 (2012).

hackers, as hacking may result in the loss of valuable data of the public. If data gets in wrong hand will prove very costly to the economy of the country for sure. Penalties are not enough to tackle data tempering. The success or failure of the Aadhaar project remains to be determined. Even though the detailed analysis focused on biometric identification system in India, the practical application and findings of the public-private partnership can be applied in a broader perspective. Whether Aadhaar is successful or not, the outcomes and implications will be a notable indication for other nations to determine if the application of a biometric identification system should be adopted in the interests of their own residents.[214]

5.3. Emergence of the issue of Data Privacy or Data Protection

The protection of data finds its roots in the individual's right to privacy doctrine.The rise in the concepts such as modern media, technological advancements and the issues relating to those which are discussed above, have hugely demanded the data protection or data privacy law in a country to protect the information of its individual subjects and from privacy being getting violated. As it has been discussed in the former chapter of this dissertation, there are many aspects to the privacy of a person, which may be related to privacy of one's communication, privacy of body, privacy of home and privacy of one's own record. There are certain aspects which can be left with the judicious interpretation of the judiciary, but with today's techno-centric era the data or records of any individual are highly unsafe and always in the verse of getting violated. Hence, a strong need is required for a data protection or privacy legislation through which specific grounds will be engraved and stated, as perthe instances on which any privacy right of an individual will be considered as violated and which will positively and absolutely inherit the right of getting relief or being implemented in the Court of law.

India does not currently have a specific data protection law. Data protection and privacy are given scattered and rather sparse coverage by existing laws. The existing data protection laws, discussed in some detail below, are strewn in laws pertaining to information technology, intellectual property, crimes, and contractual relations.Under

214 *Id.*

increasing pressure from BPO operations and call centres in India that handle large volumes of data from the United States and Europe, the Indian government is contemplating the passage of a comprehensive law protecting data.[215] Despite the urgency of the matter and pressure from internal and external fronts, India has delayed enactment of legislation for several years.[216] The form of the legislation, whether umbrella, sectoral, or a combination of the two, which will provide optimal protection for cross-border data processed in India, has been under discussion for several years. At this point, it appears likely that India's *Information Technology Act* of 2000 (hereinafter referred as IT Act of 2000) will be amended to incorporate laws that provide comprehensive protection to data. This approach, which continues to be discussed as the probable solution to India's data protection dilemma, does not entail enactment of a separate comprehensive law to deal with data security and privacy issues across all industries, as has been the case with the European Union[217] and other such countries, respectively.

Until there will be a time when there will be laws enacted for data protection, currently India adopts a system where protection is provided only when there is a data violation. These existing laws, including the *IT Act* of 2000, which is the most pertinent since it pertains specifically to the use of computer data and few provisions which deals with data protection and privacy.Some of the provisions are Section 43 A of the Act which states where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, not exceeding five crore rupees, to the person so affected.[218] Also, Section 72 A of the act provides for the

---

215 Andy McCue, *Offshore Data Protection Law Flounders*, SILICON.COM (June 10, 2018), http: /www.silicon, coml. research /special reports/offshoring/0.3S00003026.39130054.00.html.

216 *Id.* "An amendment to the IT Act of 2000, offering enhanced protection to data, was close to enactment in 2004, after 7 years in the making; unfortunately, this proposed amendment was shelved due to a change of India's Central Government".

217 Another alternative that was discussed, but is unlikely to be enacted, is an "umbrella" data privacy law similar to the E.U. Directive, which allows for sectoral adjustments. This proposal would encompass the E.U.'s comprehensive and expansive legislation, while retaining the flexibility of the U.S.'s sectoral approach. This proposal was offered by Rodney Ryder, a member of the committee considering data privacy/protection laws in India.

218 Information Technology Act, Sec. 43 A (2000).

punishment for disclosure of information in breach of lawful contract.[219] In 2011, the government enacted the *Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules*, 2011 for the better explanation of provisions of the Act.[220]

Apart from the above legislation, there is *Right to InformationAct* of 2005 (hereinafter referred as RTI Act) which gives a fair chance for protection of one's privacy rights and personal as well as public information. The RTI Act was designed to promote transparency in government, not to permit the invasion of the privacy of individuals who use government hospitals or who altruistically participate in government-funded research. There are specific provisions[221] in the Act which speaks for the protection of privacy rights of an individual. However, it is very important to note here that these enactments are not adequate for data privacy or data protection and to a very minimal level it protects the privacy rights of an individual.

5.4. Conclusion

In India the Government proposes to bring out a legislation that will provide protection to individuals in case their privacy is breached through unlawful means. For these purpose it worked on the *Right to Privacy Bill* of 2011[222] where the drafting of the legislation is at a very preliminary stage and details of the legislation are yet to be finalized.[223] Even though such attempts were made by the government, no solid result in the form of absolute positive privacy legislation has been enacted by the legislature, which gives the perpetrators to do wrongful acts with the information of the individuals for its own wrongful gain. The rise in the concepts such as modern media, technological advancements and the issues relating to those which are discussed above, have hugely

---

219 Information Technology Act, Sec. 72 A (2000).

220 Aashit Shah and Nilesh Zacharias, *Data privacy and Data Protection*, NISHITH DESAI ASSOCIATES5, 1-11 (2001).

221 Section 8(1) entitled "What is not open to disclosure", the Act says that "(j) information which relates to personal information the disclosure of which has no relationship to any public activity or interest, or which would cause unwarranted invasion of the privacy of the individuals should not be disclosed." In addition, the same section stipulates that "(e) information available to a person in his fiduciary relationship, such as the relationship of a physician or researcher with a patient or subject-should not be disclosed "unless a competent authority is satisfied that the larger public interest warrants the disclosure of such information."

222 *Draft Bill on Right to Privacy*, MINISTRY OF HOME AFFAIRS, Government of India, https://cis-india.org/ internet-governance/draft-bill-on-right-to-privacy (September 29, 2011).

223 *Id.*

demanded the data protection or data privacy law in a country to protect the information of its individual subjects and from privacy being getting violated. As it has been discussed in the former chapter of this dissertation, there are many aspects to the privacy of a person, which may be related to privacy of one's communication, privacy of body, privacy of home and privacy of one's own record. There are certain aspects which can be left with the judicious interpretation of the judiciary, but with today's techno-centric era the data or records of any individual are highly unsafe and always in the verse of getting violated. Hence, a strong need is required for a data protection or privacy legislation through which specific grounds will be engraved and stated, as per the instances on which any privacy right of an individual will be considered as violated and which will positively and absolutely inherit the right of getting relief or being implemented in the Court of law.

CHAPTER 6

CONCLUSION AND SUGGESTIONS

In India, the right to privacy is not a positive right. It comes into effect only in the event of a violation. The law on privacy in India has primarily evolved through judicial intervention. It has failed to keep pace with the technological advancement and the burgeoning of the 24/7 media news channels. The prevalent right to privacy is easily compromised for other competing rights of 'public good', 'public interest' and 'State security', much of what constitutes public interest or what is private is left to the discretion of the media.Reflecting on the volume of case law in India on privacy, one is struck at once, both by the elasticity of the concept of privacy, spanning, as it does, diverse fields from criminal law to paternity suits to wiretapping, as well as its fragility, the flag of privacy is constantly being raised only to be ultimately overridden on pretexts that range from security of state, to a competing private interest.

On the one hand, one marvels at the success of the concept, only a few decades old in Indian law, in insinuating itself into legal arguments across diverse contexts. On the other hand, one is dismayed by the fact that rarely does the concept seem to score a victory. There is an almost ritual quality to the way in which the 'right to privacy' is invoked in these cases, always named as a relevant factor; it never seems to substantially influence the outcome of the case at hand. The right to privacy in India was an 'Oops' baby, bom on the ventilator of a minority decision of the Supreme Court, and nourished in the decades that followed by sympathetic judges, who never failed to point out that this right was contingent, not absolute, not meant to be under the Constitution, but carved out anyway. Some five decades after its first invocation by the Supreme Court, one gets the feeling that the right to privacy, conceptually, hasn't moved, and is still what it was then. We don't, today, for the many times it has been invoked by courts, have a thicker, more robust concept of privacy than we started out with. So the question, that one is stuck with is, what work does this concept of privacy do and how important it is to protect this as a right?

One of the failings of the concept of privacy in India is that it doesn't exist as a positive right, but is merely a resistive right against targeted intrusion. So for instance,

the right to privacy would be useless as a concept to resist something like generalized street video surveillance, as long as a citizen is not singled out for a disadvantage, this right would be of no use. So this right to privacy is a negative right to not be interfered with. Under it one does not have the right to be as private as one wishes, but only no less than the next person. Still, even this limited concept could be useful, if it were applied more rigorously.One may perhaps add judicial inactivity as one of the limiting factors on privacy. By holding that violations of procedure by investigating agencies would not vitiate trials, the judiciary has been complicit in perhaps some of the more damaging incursions into privacy. Once a person is implicated in any manner in the criminal justice system, either as a victim, a witness or an offender, investigating agencies are immediately invested with plenary powers. They can search his house without warrant. They can place him arrest. Subject him to 'medical examinations' take his fingerprints and DNA and hold it in a bank and there is nothing you can do. In this context, perhaps the strongest privacy safeguard can come from a reform in criminal procedure alone.

Privacy is an individual as well as a social value. It is undoubtedly invaded everywhere at every moment due to the application of scientific and technological advances. Invasion of privacy and copyright violations are more in cyberspace in the form of violation of data protection, though it is invisible. It has become very difficult to keep confidential information, communications anonymity etc., due to media interferences and rapidtechnological advancements. Piracy is lucrative business now-a-days. However, the laws lag behind the digital revolution.Hence, there is a strong requirement for the formulaion of alaw which will be absolute in its nature, to give validity to the privacy rights of the people and to prevent it from unwanted intrusion. Hence therefore, the aforementioned discussion and the analysis of the respective chapters of the dissertation proves both the hypotheses where the first states that if unchecked, the repercussions of the overreaching powers of a techno-friendly society and privacy-destroying technologies shall lead us to the naked society, where privacy will be zero and where the privacy right will rarely survive. It is very difficult all the time to rely upon the decision of the judiciary for making privacy rights existent or valid. Therefore, it proves the second hypothesis that the right to privacy as a right is not protected to a great magnitude in the country of India as there exist no concrete absolute positive law to support its existence.

Judiciary for ages is doing a veracious job in justifying the importance of the privacy rightin India by carving the meaning within the fundamental right of the Constitution. But the part cannot be denied that ultimately its within the discretionary authority of the judiciary, who if public interest and state security requires can deny this right to any individual. Henceforth, an absolute positive law of privacy is required to secure such rights from getting violated and intruded by individuals, governmental and non-governmental enterprises for its own wrongful unjust enrichments. A law which is in its contrete form and provisions of which if violated, will need no discretion to sentence it whether it was a violation or not, and which will be directly enforceable in the Court of law.

Suggestions

Considering that the international community regards the right to privacy and data protection as a basic human right, India may be under a moral as well as legal obligation, being signatories to many such international instruments, to enact privacy and data protection regulations. There are two modes in which regulations can be adopted: Self-regulation and Government regulation.

a) Self-regulation: India could consider promoting an initiative among Indian industries, especially those interested in the growth of e-commerce. Self- regulation by the industry offers the advantage of a flexible policy made by those who know the trade practices and are motivated by the desire of customers. Self- regulation is also cost efficient to the government, as enforcement mechanisms need not be established. However, a large and heterogeneous group of agents may make self-regulation difficult. However, there is also the risk that self- regulatory solution would be to set the lowest standard.

b) Government Regulation: Alternatively, the Indian government could adopt specific legislation to address privacy and data protection issue. Even countries like the US that have primarily taken a self-regulatory approach to protecting privacy on the

Internet, are slowly moving towards Government regulation to bring about uniformity and effective application of privacy standards.[224]

Considering the above orbligations and international instruments, if India decides to enact the privacy law in the country, there are specific issues which are required to be considered during the formulation of such laws**.**Tallied and given below are some of the specific issues which the Indian government should keep in mind before drafting a privacy legislation.Firstly, protection from arbitrary and unlawful interference by the Government and private parties should be scrutinized. The legislation must ensure that an individual's right to privacy is not interfered with in an arbitrary and unlawful fashion. Presently, judicial precedents prohibit violation of the right to privacy of an individual by Government agencies. A comprehensive law must provide for protection from intrusion by the Government as well as private parties, where the law must also address issues relating to trespass upon individual privacy, audio and video surveillance and interception of communications (including digital and electronic communications).[225]

The legislators must also try and prohibit/curtail the use of cutting-edge technology to trespass upon privacy rights and personal data. Presently, the right to privacy on the Internet is being threatened due to several elements such as web cookies[226], unsafe electronic payment systems[227], Internet service forms[228],

---

224 H. W. R. WADE & C. F. FORSYTH, ADMINISTRATIVE LAW (Oxford University Press, 9th ed., 2004).

225 Shah, *supra* note 221, at 8.

226 A Cookie is a message given to a Web browser by a Web server. The browser stores the message in a text file called cookie.txt. The message is then sent back to the server each time the browser requests a page from the server. Cookies were initially designed to address the fact that Web sites didn't know whether a user is a first time or repeat visitor, and possibly prepare customized Web pages for them. The information placed in a cookie is not only useful in the context of e-commerce but cookies provide marketing information; they can track the ads that have been clicked on, in order to provide internet users with similar banner ads in the future. Cookies are a source of concern relating to privacy on the Internet, because of the ability to track the activities of users without their knowledge (June 18, 2018), http://www.cookiecentral.com/faq/.

227 While purchasing anything on the Internet a consumer is required to use a credit card. This results in the transmission of a credit card number over the Internet, which is very sensitive personal data and the concern is that this information will then be re-used for another purpose or sold to direct marketers. Consumers are three to four times more likely to experience theft or misuse of their credit cards when they shop online. ('Jupiter Media Metrix report on e-commerce fraud' by Jim Van Dyke) Part of the problem is that some web site owners don't understand how to secure their sites properly or how to hire skilled staff, or they lack the funding necessary to provide adequate security measures to ensure privacy protection.

browsers[229]and spam mail[230]. And also protected schemes like Aadhaar is not prevented from such intrusion or trespass with the strong modern media and technological advancements. Hence, the prohibition of technology which lead to violation of the privacy rights must be mandated in the following legislation.[231]

Thirdly, protection of medical records is also one of the important aspect for the prevention of the privacy rights of an individual under the head of privacy of one's body. Historically, medical records were used largely by physicians and medical insurers. However, with the creation of electronic records and large databases of medical information, the number of health care professionals and organizations with access to medical records has increased. While such availability allows for research that can improve the understanding of diseases and treatments across broad populations, the number of parties with routine access to personally identifiable medical data has raised concern about the potential misuse of this data. It is essential that such data is not collected and sold to researchers in the field biomedical science, without the consent of the patients. With the advent of the internet, it has become increasingly difficult to track such data and not only does it amount to an invasion of privacy, but it also amounts to breach of the duty of confidentiality that medical professionals owe to their

---

228 While subscribing to most Internet services, or gaining membership to online clubs Web sites require visitors to provide some extremely personal information, without offering any assurance with regards to privacy of that information. To join, users are almost always required to give their name, address, telephone number, e-mail address, products bought etc. The primary purpose of gathering personal information about consumers is market research. The information collected helps online businesses to understand consumer trends and helps them target their consumers more effectively. This personal information is either used by the business collecting it or is often sold to other businesses with a view to getting direct access to the consumers they wish to target.

229 An Internet Browser interprets HTML the programming language of the Internet, into the words and graphics that are seen my Internet users when viewing a web page. It is a type of software that allows Internet users to navigate information databases. There have been many reports of security bugs in browsers, which can enable web sites to access your personal information while a person is surfing the web. Most manufactures of Internet browsers have attempted to fix the bugs to prevent access to sensitive personal data of the users of such browsers. However, the threat still persists and browsers could result in the leakage of information such as the e-mail address or username of the Internet user (June 18, 2018), http:// www.cen.uiuc .edu /~ ejk /WWW-privacy.html.

230 Spam is the use of e-mail addresses for a purpose that consumers have not consented for and constitute a violation of personal rights. Internet users who have purchased a product over the Internet or have their e-mail address published on a web site or have subscribed to a news service or who have participated in news groups or mailing lists, often receive unsolicited / spam e-mail. Some Internet Service Providers and other Internet businesses engage in the unlawful practice of selling lists of their customer's e-mail addresses to other companies. These companies use programs to generate bulk e-mail messages that are intended to advertise or promote a business, web site or product.

231 Shah, *supra* note 221, at 8.

patients.[232]Then again protection of financial records of individuals must also be considered from being distributed and circulated among banks and financial companies as it may also result in the misuse of such information and also preventing excessive monitoring of employees by the employer is another major concern which shall be given due consideration.[233]

Considering the issues illustrated above while drafting a privacy law in India, the government can further adopt certain principles which are internationally recognised for the better and concrete formulation of the law. These principles are based on the "*Safe Harbour Principles* adopted between EU and US.

a) Notice: The data subject must be given notice in clear language, when first asked for personal data, of the purpose of data collection, the identity of the data controller, the kinds of third parties with whom the data will be shared, how to contact the organization collecting or processing the data, and the choices available for limiting use or disclosure of the information.

b) Choice: The data subject must be given clear, affordable mechanisms by which he or she can opt out of having personal information used in any way that is inconsistent with the stated purposes of collection.

c) Onward transfer: Where the data controller has adhered to the principles of notice and choice, it may transfer personal data if it ascertains that the receiving party also complies with the safe harbour principles, or if it enters into a contractual agreement that the receiving party will guarantee at least the same level of data protection as the transmitting party. When disclosure is made to a third party that will perform under instructions of the data controller, it is not necessary to again provide notice or choice, but the onward transfer principle continues to apply.

d) Security: The data controller must take reasonable precautions to protect data from loss or misuse, and from unauthorized access, disclosure, alteration or destruction.

---

232 *US Report to Congressional Requesters on Medical Records Privacy*, www.epic. org/ privacy /medical /gao-medical-privacy-399.pdf. (last updated January 21, 2013).

233 *Id.*

e) Data integrity: The data controller must take reasonable steps to ensure that data are accurate, complete and current.

f) Access: Data subjects must have reasonable access to their personal data and an opportunity to correct inaccurate information.

g) Enforcement: At minimum, enforcement mechanisms must include readily available and affordable recourse for the investigation of complaints and disputes, damages awarded where applicable, procedures for verifying the truthfulness of statements made by the data controller regarding its privacy practices, obligations of the data controller to remedy problems arising out of noncompliance, and sanctions sufficiently rigorous to ensure compliance."[234]

Currently,the existent legal system is ineffective in addition to being ill-equipped to protect the privacy of citizens. The absence of appropriate statutory measures for the protection of privacy rights in India is becoming of greater concern to investors, corporations, the legislature, and the public in other nations.[235] India is being urged to enact an adequate at a protection regime which dictates the appropriate parameters for the collection, storage and use of personal data by private and government entities. Given the international focus on India's data protection scheme, it is merely a matter of time before India enacts data protection laws. However, since intellectual property rights that lack enforcement are worthless, the seminal issue that remains once the data protection laws are in place is whether the laws will be enforced in such a manner as to provide any meaningful protection to data. The existing enforcement regime in India's legal system is pitifully deficient, marred by interminable delays in moving matters through the existing court system. India will be unable to provide adequate protection to data unless a solution is found to address the court

234 Shah, *supra* note 221, at 9.

235 John Ribeiro, *Indian Law may satisfy EU Data Protection Concerns*, COMPUTER WORLD, http://www. computerworld.eom/printthisI2004/0,4814,92557,00.html (last updated April 21, 2004).

delays, and procedures established for expediently prosecuting data protection breaches and compensating those harmed.[236]

Furthermore, once the data protection laws in India are strengthened, the general legal system must also be tweaked with an alternative legal enforcement regime, in order to address data protection enforcement. Proposed remedies to fix the enforcement void include establishment of a national centralized enforcement body dedicated to, and trained in, electronic data privacy and enforcement. This national body must be given jurisdictional authority to enforce across state borders. In addition, it is essential to have specialized local police enforcement units which are specifically trained and maintained to recognize instances of, and enforce actions against, data piracy crimes. Finally, it is vital to adopt meaningful court reform to decrease burdens, costs and delays, and ensure that cases are concluded promptly with deterrent penalties and damages. Specialized judicial avenues of enforcement are the logical transition that India must make due to the inability of the regular court system in India to deal with the additional volume of cases that cross-border crimes will generate. The solution is the establishment of specialized cyber infringement courts with jurisdiction overall violations related to intellectual property, including data privacy, where the specific model for such a court will depend on factors such as local customs and practices (including local procedural considerations), cyber infringement case loads, number of judges, and monetary considerations.[237]

---

236 Robert M. Sherwood, *The TRIPS Agreement: Implications for Developing Countries*, 37 IDEA 491 (1996-1997).

237 Shah, *supra* note 221, at 10.

BIBLIOGRAPHY

PRIMARY SOURCES

Acts

Constitution of India, 1950

India Post Office Act, 1898.

Indian Evidence Act, 1872.

Information Technology Act, 2000.

Information Technology Act, 2008.

Medical Termination of Pregnancy Act, 1971.

Right to Information Act, 2005.

The Code of Criminal Procedure, 1973.

The Indian Telegraph Act, 1885.

Commissions, Conventions and Reports

African Charter on the Rights and Welfare of the Child, 1990.

African Union Principles on Freedom of Expression (the right of access to information), 2002.

American Convention on Human Rights, 1969.

American Declaration of the Rights and Duties of Man, 1948.

Arab Charter on Human Rights, 1994.

ASEAN Human Rights Declaration, 2012.

European Convention on Human Rights, 1950.

International Covenant on Civil and Political Rights, 1976.

UN Convention on the Rights of the Child, 1989.

United Nations Convention on Migrant Workers, 1994.

Universal Declaration of Human Rights, 1948.

Justice Manepalli Narayana Rao Venkatachalliah Commission, 2000.

Cases

US and UK Cases

Albert v. Strange, 1 Mac & G 25: 41 ER 1171 (1849).

Bowers v. Hardwick, 478 US 186 (1986).

Carey v. Population Services International, 431 US 678, 685 (1977).

Eisenstandt v. Baird, 405 U.S. 438 (1972).

Griswold v. Connecticut, 381 U.S. 47 (1965).

Kats v. United States, 389 U.S. 347 (1967).

Katz v. United States, 389 U.S. 347 (1967).

Kaye v. Robertson, FSR 62 (1991).

Lawrence v. Texas, 539 US 558 (2003).

Loving v. Virginia, 388 U.S. 1 (1967).

Meyer v. Nebraska, 262 US 390 (1923).

Olmstead v. United States, 277 U.S. 438 (1928).

Pierce v. Society of Sisters, 268 US 510 (1925).

Prince v. Massachusetts, 321 US 158 (1944).

Roe v. Wade, 410 US 113 (1973).

Skinner v. Oklahoma, 316 US 535 (1942).

Stanley v. Georgia, 394 US 557 (1969).

Thornburgh v. American College of Obstetricians & Gynecologists, 476 US 747, 772 (1986).

Washington v. Glucksberg, 521 US 702 (1997).

Indian Cases

Bhabani Prasad Jena v. Convenor Secretary, Orissa State Commission for Women & Another, AIR 2851 (SC 2010).

District Registrar and Collector, Hyderabad v. Canara Bank, SCC 496 (1 SC 2005).

Goutam Kundu v. State of West Bengal and Another, AIR 2295 (SC 1993),1993 SCR (3) 917.

Govind v. State of Madhya Pradesh, AIR 1376 (SC 1975).

Hukam Chand Shyam Lal v. Union of India and others, AIR 789 (SC 1976), 1976 SCR (2)1060, (1976) 2 SCC 128.

Justice K.S Puttaswamy (Retd.) v. Union of India, Writ Petition(s) (Civil) No(s). 494/2012.

Kharak Singh v. State of U.P, AIR 1925 (SC 1963).

M.P. Sharma v. Satish Chandra, SCC 300 (SC 1954).

Maharashtra v. Natwarlal Damodardas Soni, AIR 593 (SC 1980),1980 SCR (2) 340.

Maneka Gandhi v. Union of India, AIR 597 (SC 1978).

Mr. X v. Hospital Z, SCC 500 (1 SC 2003).

Ms. X v. Mr. Z and Another, AIR 217 (Delhi 2002).

Ponnenvs M.C. v. Varghese, AIR 228 (Ker. 1967), 1967 Cri.L.J. 1511.

PUCL v. Union of India, AIR 568 (SC 1997).

R. M. Malkani v. State of Maharashtra, AIR 157 (SC 1973); 1973 SCR (2) 417.

R. Rajagopal v. State of Tamilnadu, AIR 632 (6 SC 1994), 649-50.

Radhakrishan v. State of U.P., Supp. 1 S.C.R. 408 (1963).

Ramchandra Ram Reddy v. State of Maharashtra, 1 (2205) CCR 355 (DB).

Romesh Thappar v. The State of Madras, AIR 124 (SC 1950), 1950 SCR 594.

Selvi v. State of Karnataka, SCC 263 (7 SC 2010).

Sharda v. Dharmpat, AIR 493 (4 SC 2003).

Shri Rohit Shekhar v. Shri Narayan Dutt Tiwari, 23 December, 2010.

State of Bombay v. Kathi Kalu Oghad and Ors., AIR 1808 (SC 1961).

State of U.P. v. Kaushaliyal and others, AIR 416 (SC 1964).

State of U.P. v. Ram Babu Misra, AIR 791 (SC 1980), 1980 SCR (2)1067, (1980) 2 SCC 343.

Suchita Srivastava v. Chandigarh Administration, AIR 1 (9 SC 2009).

Suresh Kumar Koushal and Others. v. Naz Foundation and Others, SCC (Cri. 1) (4 SC 2013).

Thogorani Alias K. Damayanti v. State of Orissa and Ors., 2004 Cri L J 4003 (Ori).

Unique Identification Authority of India & another v. Central Bureau of Investigation, Special Leave to Appeal, (Crl.) No(s).2524/2014.

SECONDARY SOURCES

Books

2 BASU, DURGA DAS, COMMENTARY ON THE CONSTITUTION OF INDIA (Lexis Nexis, 3rd ed. 2016).

ALAN F. WESTIN, PRIVACY IN INDIA, (1994).

ARISTOTLE, B. JOWETT AND H.W.C. DAVIS, ARISTOTLE'S POLITICS (Clarendon Press 1908).

COLIN J. BENNETT & CHARLES D. RAAB, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE (2003).

D.D. BASU, SHORTER CONSTITUTION OF INDIA (Wadhwa, Nagpur 2004).

D.K. SINGH, V. N. SHUKLA'S CONSTITUTION OF INDIA (Eastern Book Company, Delhi, 7th ed. 1982).

H. W. R. WADE & C. F. FORSYTH, ADMINISTRATIVE LAW (Oxford University Press, 9th ed. 2004).

HUEBERT, RONALD, PRIVACY IN THE AGE OF SHAKESPEARE (University of Toronto Press 2015).

J. L. MILLS, THE LOST RIGHT (Oxford University Press 2008).

J.A. CANNATACI, THE INDIVIDUAL AND PRIVACY (Routledge 2015).

J.N. PANDAY, CONSTITUTIONAL LAW OF INDIA (Central Law Agency, Allahabad, 37th ed. 2001).

JUSTICE YATINDRA SINGH, CYBER LAWS (Universal Law Publishing, 6th ed. 2016).

M. GLENN ABERNATHY, CIVIL LIBERTIES UNDER THE CONSTITUTION (1977).

M.P. JAIN, INDIAN CONSTITUTIONAL LAW (LexisNexis Butterworths Wadhwa Nagpur, 6th ed. 2010).

P.M. BAKSHI, THE CONSTITUTION OF INDIA (Universal Law Publication, Delhi 2009).

PARAS DIWAN, ADMINISTRATIVE LAW (Allahabad Law Agency 2004).

RAYMOND WACKS, PERSONAL INFORMATION: PRIVACY AND THE LAW (Clarendon Press 2003).

RICHARD A. GLENN, THE RIGHT TO PRIVACY: RIGHTS AND LIBERTIES UNDER THE LAW (ABC-CLIO, Inc., 2003).

Journals

A.S. Popkin Helen, *Govt. officials want answers to secret iPhone tracking*, MSNBC TECHNOLOGY (2011).

Aashit Shah and Nilesh Zacharias, *Data privacy and Data Protection*, NISHITH DESAI ASSOCIATES (2001).

Abhinav Chandrachud, *The Substantive Right to Privacy: Tracing the Doctrinal Shadows of the Indian Constitution,* 3 S.C.C. (Jour.) (2006).

Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. (1994).

Archana Parashar, *Right to have Rights: Supreme Court as the Guarantor of Rights of Persons with Mental/ Intellectual Disability*, 5 THE INDIAN JOURNAL OF CONSTITUTIONAL LAW (2011).

Charles Fried, *Privacy*, 77 YALE L.J. (1968).

Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. (2002).

Gautam Swarup, *Why Indian Judges would Rather be Originalist: Debunking Practices of Comparative Constitutional Law in India*, 5 INDIAN JOURNAL OF CONSTITUTIONAL LAW (2011).

Glenn Negley, *Philosophical Views on the value of Privacy*, 31 LAW & CONTEMP. PROBS. (1966).

Greenleaf Graham, *Global Data Privacy Laws: 89 Countries, and Accelerating*, Social Science Electronic Publishing, 98 QUEEN MARY SCHOOL OF LAW LEGAL STUDIES (2012).

Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 7 LAW & PHIL. (1998).

James Rachels, *Why Privacy is Important?* 4 PHIL. & PUB. AFF. 326, 323-340 (1975).

Jed Rubenfield, *The Right to Privacy*, 102 HARV. L. REV. (1989).

Lohit D.Naikar, *The Law Relating to Human Rights*, BANGALORE PULANI AND PULANI (2004).

Madison Powers, *A Cognitive Access Definition of Privacy*, 15 LAW & PHILO. (1996).

Manoj Krishna, *Privacy Revisited*, 24 THE ACADEMY LAW REVIEW (2000).

Milton R. Konvitz, *Privacy and Law: Philosophical Prelude*, 31 LAW AND CONTEMPORARY PROBLEMS (1966).

Praveen Kumar and Chander Kant, *Unique Identification System in India: A Big Challenge*, 5 INTERNATIONAL JOURNAL OF INFORMATION TECHNOLOGY AND KNOWLEDGE MANAGEMENT (2012).

Privacy in the Digital Environment, HAIFA CENTRE OF LAW & TECHNOLOGY (2005).

R. Revathi, *Pervasive Technology, Invasive Privacy and Lucrative Piracy*, 51 JILI (2009).

Robert M. Sherwood, *The TRIPS Agreement: Implications for Developing Countries*, 37 IDEA (1996-1997).

Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 437 (1980).

Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. (1890).

Satya Vrat Yadav and Vasundhara Anil Kaul, *Right to Privacy: Redefining Social Security in India*, 3 INTERNATIONAL JOURNAL OF LAW AND LEGAL JURISPRUDENCE STUDIES (2012).

Subhajit Basu, *Policy-making, Technology and Privacy in India*, 6 THE INDIAN JOURNAL OF LAW AND TECHNOLOGY (2010).

Suhrith Parthasarathy, *Privacy, Aadhaar and Constitution,* THE HINDU CENTRE FOR POLITICS AND PUBLIC POLICY (2017).

Tom Gerety, *Redefining Privacy*, 12 HARV. C.R.C. L. L. REV. (1977).

Ujwala Uppaluri & Varsha Shivanagowda, *Preserving Constitutive Values in the Modern Panopticon: The Case for Legislating toward a Privacy Right in India*, 5 NUJS L. REV. (2012).

Utkarsh Amar, *Right to Privacy in the Dawn of Information and Communication Technology- A Critical Review*, 3 INTERNATIONAL JOURNAL OF LAW AND LEGAL JURISPRUDENCE STUDIES (2012).

Web Sources

Andy McCue, *Offshore Data Protection Law Flounders*, SILICON.COM (June 10, 2018), http:/www.silicon, coml. research /special reports/offshoring/0.3S0000302 6.39130054.00.html.

Anon, *2010 High Court dismisses appeal seeking information on Sonia Gandhi's religion*, NDTV ONLINE, (June 21, 2018), http://www.ndtv.com/article/india/high-court-dismisses-appeal-seeking-informationon-sonia-gandhi-s-religion-69356.

Bonnie Lowenthal, *AB-1291 Privacy: Right to Know Act of 2013: disclosure of a customer's personal information*, (June16,2018), http://leginfo.legislature.ca.gov/ faces/ billNavClient.xhtml?billid=201320140AB129.

CIC/OK/A/2008/987/AD, December 22, 2008 (June 22, 2018), http:// indiankanoon.org/doc/1479476/.

Concept, Unique Identification Authority of India, http://uidai.gov.in/uid-brand/concept.html (last updated June 10, 2016).

Dativa, *Adopting a Virtual Data Protection Officer*, (June 11, 2018) https://www.dativa.com/virtual-dpo/.

Draft Bill on Right to Privacy, MINISTRY OF HOME AFFAIRS, Government of India, https://cis-india.org/internet-governance/draft-bill-on-right-to-privacy (Sept 29, 2011).

Frontier Technology, *The difference between EU and US data laws*, (June 116, 2018) http://www.frontiertechnology.co.uk/about-us/news/differences-between-eu-and-us-data-laws/.

J. Venkatesan, *Don't tie up benefits to Aadhaar: Court tells Centre*, THE HINDU (June 15, 2018) http://www.thehindu.com/todayspaper/tp-national/dont-tie-up-benefits-to-aadhaar-court-tells-centre/article5162 837.ece.

John Ribeiro, *Indian Law may satisfy EU Data Protection Concerns*, COMPUTER WORLD, http:// www.computerworld.eom/printthisI2004/0,4814,92557,00.html (last updated April 21, 2004).

K. R Srivats, *Aadhaar legislation tabled as a money Bill*, THE HINDU (June 15, 2018),http://www.thehindubusinessline.com/economy/new-aadhaar-bill-introduced-as-money-bill-in-lok-sabha/article 8309587.ece.

M. N. Venkatachaliah, *Fundamental Rights, Directive Principles and Fundamental Duties*, REPORT OF THE NATIONAL COMMISSION TO REVIEW THE WORKING OF THE CONSTITUTION, 2002, http://lawmin.nic.in/ncnvc/final report/vlch3.html (last updated January 19, 2013).

Marc Rotenberg, *The Privacy Law Sourcebook*, EPIC 1999, (June 20, 2018), http://www.epic.org/bookstore/pls.

Prashant Iyengar, *Limits to Privacy*, CIS/PRIVACY INDIA, http://ssm.com/ abstract=l807733 or http://dx.doi.org/10.2139/ssm.1807733 (April 12, 2011).

Protecting and Promoting Privacy Rights, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, https://www.priv.gc.ca/en/ (last updated February 16, 2014).

Sarai Reader 07: Frontiers, and nothing but the truth, so help me science, DELHI: CSDS, Delhi, 100-110, (June 20, 2018),http://www.sarai.net/publications/ readers/07-frontiers/100- 10_lawrence.pdf.

The Federal Council's Message to Parliament, 19 BBl 2101, https://www.admin.ch/opc/de/federal-gazette/2003/2101.pdf (last updated 2003).

Thomas, Kendall, *Beyond the Privacy Principle*, 92 COLUM. L. REV. (1992); Yoshino, Kenji, Sodomy Laws: Law of the Bedroom, BOSTON GLOBE (Mar. 23, 2003), http://www.kenjiyoshino.Com/articles/law_of_the_bedroom_sodomy_laws .pdf.

Unique Identification Authority of India, http://www.uidai.gov.in/images/ notification28jan2009.pdf (last updated June 10, 2016).

US Report to Congressional Requesters on Medical Records Privacy, www.epic. org/ privacy /medical /gao-medical-privacy-399.pdf. (last updated January 21, 2013).