The National University of Advanced Legal Studies, Kochi

DISSERTATION

Submitted in partial fulfilment of the requirement for the award of the degree of

MASTER OF LAW (LL.M)

(2020-2021)

ON THE TOPIC

PRIVACY AND DATA PROTECTION IN CYBERSPACE – A CRITICAL ANALYSIS OF DATA PROTECTION LAWS IN INDIA

Under the guidance and supervision of

Dr. Sandeep M.N.

Assistant Professor

NUALS

Submitted by

Ann Maria Sebastian

Reg No-LM0120003

LLM (Constitutional and Administrative Law)

CERTIFICATE

This is to certify that Ms. ANN MARIA SEBASTIAN, REG N0-LM0120003 has submitted her dissertation titled "PRIVACY AND DATA PROTECTION IN CYBERSPACE – A CRITICAL ANALYSIS OF DATA PROTECTION LAWS IN INDIA" in partial fulfilment of the requirement for the award of Degree of Masters of Laws in Constitutional Law and Administrative Law to the National University of Advanced Legal Studies, Kochi under my guidance and supervision. It is also affirmed that the dissertation submitted by her is original, bona fide and genuine.

Dr. Sandeep M.N.

Guide and Supervisor
NUALS, Kochi

Date:
Place: Ernakulam

DECLARATION

I declare that this dissertation titled "PRIVACY AND DATA PROTECTION IN CYBERSPACE – A CRITICAL ANALYSIS OF DATA PROTECTION LAWS IN INDIA" is researched and submitted by me to the National University of Advanced Legal Studies, Kochi in partial fulfilment of the requirement for the award of Degree of Master of Laws in Constitutional Law and Administrative Law, under the guidance and supervision of Dr. Sandeep M.N., Assistant Professor. It is an original, bona fide and legitimate work pursued for an academic interest. This work or any type thereof has not been submitted by me or anyone else for the award of another degree of either this University or any other University.

Ann Maria Sebastian

Reg No-LM0120003

LLM (Constitutional and Administrative Law)

Date:

Place: Ernakulam

ACKNOWLEDGEMENT

I thank Almighty for His countless blessings. This dissertation is the result of the pertinent efforts and contributions of many a people around me. I have taken sincere efforts to complete the dissertation, enjoying most of the research works, finding clueless amidst and finally relieved, proud and content to complete it. First, I would like to thank, Dr. Sandeep M.N, for his guidance and support. I have been going through a hard phase, if it was not for his kindness, patience and encouragement, the dissertation would have remained incomplete. I am deeply indebted for the consistent efforts Sir has taken for widening my perception and improving my work.

I express my sincere thanks to the Vice Chancellor Prof (Dr.) K.C Sunny for his constant support. I take this opportunity to thank Prof (Dr.) Mini S. who is the Director of Centre for Post Graduate Legal Studies for her support and encouragement extended during the course. I would further extend my deep-felt gratitude to all the Professors, NUALS for their guidance and support.

I would also like to convey my thanks to all the Library Staff and the Technical Staff for their timely assistance to carry out the work.

Words fall short to express my love and gratitude to my parents, friends and family members for sticking through my side all the way. I feel blessed to have this circle of well- wishers who have always known ways to keep my spirits high.

Ann Maria Sebastian

LIST OF ABBREVIATIONS

&- And

ACCC- Australian Competition and Consumer Commission

AIR- All India Reporter

Anr- Another

APP- Australian Privacy Principles

Art- Article

CAN-SPAM - Controlling the Assault of Non-Solicited Pornography and Marketing

CFAA- Computer Fraud and Abuse Act

COPPA- Children's Online Privacy Protection Act

Del- Delhi

DPA- Data Protection Act

DPD – Data Protection Directive

DPI - Digital Platforms Inquiry

e.g. – Example

ECPA- Electronic Communications Privacy Act

ed. – Edition

etc. – et cetera

EU – European Union

FCRA- Fair Credit Reporting Act

FERPA- Family Education Rights and Privacy Act

GDPR- General Data Protection Regulation

GLBA- Gramm-Leach- Bliley Act

GPS - Global Positioning System

Guj- Gujarat

HC- High Court

HIPAA- Health Insurance Portability and Accountability Act

ICCPR-International Covenant on Civil and Political Rights

ICO- Information Commissioners Office

IoT - Internet of Things

J.- Judge

Kar- Karnataka

Ker- Kerala

OECD- Organisation for Economic Co-operation and Development

Ori- Orissa

Ors- Others

Para- Paragraph

PDP Bill – Personal Data Protection Bill

Pg- Page

SC- Supreme Court

SCC- Supreme Court Cases

SLP- Special Leave Petition

UDHR- Universal Declaration of Human Rights

UK- United Kingdom

UN- United Nations

UOI- Union of India

UP- Uttar Pradesh

USA- United States of America

v. – versus

W.P. – Writ Petition

LIST OF CASES

- Roe v. Wade 410 U.S. 113
- Saroj Rani v. Sudarshan Kumar Chadha, (1984) 4 SCC 90
- Selvi v. State of Karnataka AIR 2010 SC 1974
- Sharda v. Dharmpal AIR 2003 SC 3450
- Sri Vasunathan v The Registrar General 2017 SCC Online Kar 424
- State of Karnataka v. Krishnappa, (2000) 4 SCC 75
- State of Maharashtra v. Madhukar Narayan Mardikar (1991) 1 SCC 57
- State of Maharashtra vs. Bharat Shanti Lal Shah (2008) 13 SCC 5
- State v. N.M.T. Joy Immaculate, (2004) 5 SCC 729
- Subhranshu Rout v. State of Orissa 2020 SCC Online Ori 878
- United States v. Jones 565 US 400 (2012)
- Wolf v. Colorado 338 US 25
- 'X' v. Hospital 'Z' (1998) 8 SCC 296
- Zulfiqar Ahman Khan v. M/s Quintillion, 2019 SCC Online Del 8494

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION

"**Privacy is a special kind of independence, which can be understood as an attempt to secure autonomy in at least a few personal and spiritual concerns, if necessary, in defiance of all the pressure of modern society…It seeks to erect an unbreachable wall of dignity and reserve against the entire world. The free man is the private man, the man who still keeps some of his thoughts and judgments entirely to himself, who feels no over-riding compulsion to share everything value with others, not even those he loves and trusts."**[1]

In India, the Right to privacy is held and protected as an essential part of the right to life and personal liberty under Article 21.[2] Brandies,J. observe the essence of the right to privacy as: "…solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury. The right 'to be let alone' thus represented a manifestation of an inviolate personality, a core of freedom and liberty from which the human being had to be free from intrusion."[3]

Mark Burdon in his book 'Digital Data Collection and Information Privacy Law'[4] explains how our lives are shaped by smart devices. "Our societies are increasingly populated with the smart devices that make up the 'Internet of Things'. Sensorisation of environmental spaces is unfolding at a rapid rate as we develop smart buildings such as the smart home, store or workplace. Sensorised networks and infrastructures now make our broader environments, such as the smart city, an unfolding reality. The components of the smart world should provide significant benefits. Our smarter cities will be more resource efficient and safer places to live. Our homes will understand our needs and tailor their

[1] Clinton Rossiter, 'The Free Man in the Free Society', The Essentials of Freedom.

[2]Justice K.S. Puttuswamy v Union of India, (2017) 10 SCC 1, 262

[3]Warren and Brandeis, The Right to Privacy, 5 Harvard Law Review, 193 (1890),

[4] MARK BURDON, DIGITAL DATA COLLECTION AND INFORMATION PRIVACY LAW, (Cambridge University Press, 2020)

resources more effectively to meet our demands. Our personal devices will track our moods and behaviours to shape and work out our present and future needs."[5]

After the advent of Cyberspace, anybody could access information about anything or anybody from at ease. Anybody can upload any information to Cyberspace and store it there, and it will remain forever. Our use of social media, discussions, tweets and re-tweets on Twitter, the photos and videos we have uploaded and every page we like are stored as our 'digital footprints'. Globalization has gathered wider acceptance to cyber technology across the whole world; e-commerce, e-governance, e-learning, e-courts, etc., have made the daily affairs convenient. We live in the era of Big data where algorithm monitors the activities of our digital selves. The collection, usage, storage, access, handling and disposal of these data raise the task of resolving many legal issues, of which the most fundamental one, viz., the right to privacy with respect to cyber data[6].

The current data protection laws in India are the draft Data Protection Bill, 2019, provisions of the Information Technology Act 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. The Data Protection Bill 2019 provides for the law governing data privacy, transfer, processing etc in India. However, it gives arbitrary powers to the state to access data. The Section 35 of the PDP Bill gives India's Central Government the power to exempt any government agency from the bill's requirements on the basis of security and sovereignty of the State and public order. It provides the central government with more power and clearly designates it as a party, judge, and adjudicator in its own matter. There aren't any checks and balances in place.

Section 43A of the IT Act creates a liability on a body corporate (including a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities) which possesses, deals or handles any sensitive personal data or information in a computer resource that it owns, controls or operates to pay damages by way of compensation to the persons affected.[7]IT Rules 2011 protects the sensitive personal data or information of individuals. The body corporate

[5] Ibid, Page 15

[6] Dr. Jasmine Alex,*Privacy In Cyber Space*., Livelaw, (Accessed 3 February 2021) https://www.livelaw.in/columns/privacy-in-cyber-space-157769

[7]Section 43A in The Information Technology Act, 2000

or any person who on behalf of body corporate collects, receives, possess, stores, deals or handle information of provider of information, shall provide a privacy policy for handling of or dealing in personal information including sensitive personal data or information and ensure that the same are available for view by such providers of information who has provided such information under lawful contract.[8]

Data privacy in its simplest sense means empowering the users to make their own decisions as to how their information is collected, used, stored and shared. The topic of research is of contemporary relevance as the data privacy of individuals in cyberspace are being invaded online, most often without their knowledge. The proposed Personal Data Protection Bill, 2019, would govern the data privacy regime in India, if enacted. The unbridled powers offered to the Central Government by the proposed Bill, is a question of concern of State's interference in its citizens' privacy. The eternity and universality of 'digital footprint' is an area of concern which need to be looked into. In exercising various rights for data protection in cyberspace, the borderless nature of internet possesses the question of territoriality and applicability.

1.1.RESEARCH PROBLEM

The advent of Cyberspace and its expansion as an irreplaceable part of human life has raised a concern regarding the protection of data and privacy of people in that sphere. The universality and eternity of digital footprints are posing great threat to the privacy of people. Are the laws in India adequate enough to protect the privacy of individuals relating to their personal data in Cyberspace?

1.2.SCOPE AND RELEVANCE OF THE STUDY

- The study will trace out the evolution of the right to privacy in India especially with reference to informational privacy.
- The research would analyse the challenges to data privacy in the digital era of 'smart' devices.

[8]Rule 4 of Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

- The study analyses existing laws for data privacy in various countries and advocates for an international standard of data protection.
- A critical analysis of the Personal Data Protection Bill 2019 is made to point out flaws and incompetency in its provisions and to suggest required changes to uphold privacy.
- The work throw light on how glibly, most often without knowledge, the consent for data collection is obtained and finds 'right based' approach as a better alternative for the current 'consent based' one.

1.3.OBJECTIVES

The objectives of the research are

1. To study the extent of protection of the right to privacy in cyberspace in India
2. To understand the various Indian laws related to protection of privacy of individuals relating to their personal data.
3. To specifically analyse the adequacy of the provisions of Data Protection Bill, 2019.
4. To compare the statutory framework for protection of the privacy of individuals relating to their personal data in cyberspace in various countries.
5. To understand the scope and necessity of 'right to be forgotten' and the steps taken by Indian laws to ensure its protection.

1.4.HYPOTHESIS

The privacy of individuals relating to their personal data in cyberspace is not adequately protected by the laws in India. The Data Protection Bill granting unbridled powers to the State to access data has a 'chilling effect' on the right to privacy of citizens.

1.5. RESEARCH QUESTIONS

1. What are the recent developments in India with regard to protection of right to privacy?
2. What is the extent and scope of right to privacy in cyberspace?

3. What is the legal framework on protection of Right to Privacy in Cyberspace in various common law jurisdictions?
4. How to ensure that the right to data privacy in Cyberspace is protected in the era of Big Data?
5. What are the major steps to be adopted by India in ensuring that privacy of individuals relating to their personal data is adequately protected?
6. Whether there exist any major differences in the way personal data is protected in the Data Protection Bill in India vis-à-vis GDPR?
7. What are the judicial approaches in India to protect the data privacy of individuals in Cyberspace?

1.6. METHODOLOGY

Limited by time, the methodology of this research is doctrinal. The study is an analysis of data protection laws in various jurisdictions which can be possibly carried out through doctrinal research as it includes analysis of various legislations and case laws.

The study would be based on the collection of data from primary and secondary sources. The primary sources of data would include statutes, Bills, case laws, and secondary sources would include books, journals, newspaper articles, online resources, etc. which are available relating to the concerned study.

1.7.CHAPTERISATION

- FIRST CHAPTER - INTRODUCTION

  It deals with the introduction of this paper, research design, objectives and methodology used to answer the research questions.

- SECOND CHAPTER- ORIGIN AND DEVELOPMENT OF THE RIGHT TO PRIVACY IN INDIA

This chapter traces the origin and development of the concept of privacy and the right to privacy in India. Various international legal documents, cases from various jurisdictions, position of Indian judiciary are analysed and discussed here.

- THIRD CHAPTER- DATA PRIVACY WITH SPECIAL REFERENCE TO RIGHT TO ERASURE AND RIGHT TO BE FORGOTTEN

  This chapter intend to understand the evolution of data privacy and its nuances. The chapter also focuses on right to erasure and right to be forgotten which are aspects of data privacy in detail.

- FOURTH CHAPTER - COMPARATIVE ANALYSIS OF DATA PROTECTION LAWS IN VARIOUS JURISDICTIONS

  In this chapter, the data protection laws in USA, Australia and UK are studied.

- FIFTH CHAPTER - CRITICAL ANALYSIS OF DATA PROTECTION BILL, 2019

  The penultimate chapter focuses on the data protection laws in India with special reference to the Data Protection Bill, 2019. The chapter critically analyses the proposed Bill and compare it with other effective data protection laws. It is also intended to pin point the flaws in the Bill.

- SIXTH CHAPTER - FINDINGS AND SUGGESTIONS

  The final chapter is about findings and suggestions. The findings of the study is placed and the suggestions to effectuate data protection framework in India would be stipulated.

1.8.LIMITATIONS OF RESEARCH

The research is limited to the study of data privacy in Cyberspace. Australia, USA and UK are only chosen for comparative analysis of data protection laws in various jurisdiction and this is mainly due to the preliminary assessment that there exists strong legislative framework related to data protection in cyberspace.

CHAPTER -2

ORIGIN AND DEVELOPMENT OF THE RIGHT TO PRIVACY IN INDIA

"To respect, love, trust, feel affection for others, and to regard ourselves as objects of love, trust and affection is at the heart of our notion of ourselves as persons among persons, and privacy is the necessary atmosphere for those attitudes and actions, as oxygen is for combustion." [9]

2.1. INTRODUCTION

The idea of privacy as it exists today is not entirely in black and white. The definitions and concerns about privacy have varied over time and according to national cultures and academic perspectives. The classic American definition offered by Samuel Warren and Louis Brandeis at the end of the last century was that "Privacy was the right to be let alone".[10] However, such simplistic attempt at defining privacy failed to address which aspects of personal life should be left alone, for example, there might be privacy of space, privacy of behaviour, privacy of decisions and privacy of information.

Even the Constitutions of America and India do not expressly provide privacy as a fundamental right and thereby do not attempt to define privacy. However, over the course of time, courts of both countries have, by way of various judgments recognised and read privacy to be a part of the fundamental rights.

In India, some of the earliest decisions such as ***Kharak Singh v. State of U.P***.[11], the majority decision rejected that there exists any right to privacy.[12] However, the courts in India, with time took a leaf out of the judicial activism of the American courts and began reading into the Constitution, a fundamental right to privacy by an interpretation of the right to life guaranteed under Article 21. The Supreme Court in Justice **K.S. Puttaswamy v. UOI**, [13] , held that the

[9] Charles fried, Privacy, 77 Yale L. J., Vol.77, 475 (1968)

[10] Brandeis, *supra* note 3

[11] AIR 1963 SC 1295

[12] Though the dissent by Justice Subba Rao held that privacy is an essential ingredient of liberty under Article 21 of the Constitution of India

[13] (2017) 10 SCC 1

Right to privacy is held and protected as an essential part of the right to life and personal liberty under Article 21.

2.2. EVOLUTION OF THE CONCEPT OF RIGHT TO PRIVACY

Individuals' right to privacy goes hand in hand with their freedom to regulate their own personalities. Its origins can be traced back to the idea that a human being has certain natural or inherent rights. Because natural rights are inextricably linked to human personality, they are unalienable. Without the existence of natural rights, the human element in life is unimaginable. The Greek philosopher Aristotle spoke of a division between the public sphere of political affairs (which he termed the *polis*) and the personal sphere of human life (termed *oikos*). This dichotomy may provide an early recognition of "a confidential zone on behalf of the citizen".[14] Individual lives, liberty, and estates are, as a matter of fundamental natural law, a private preserve, according to John Locke's Second Treatise of Government, published in 1690. A private preserve was created to build boundaries against outside meddling. William Blackstone wrote about "natural liberty" in his Commentaries on the Laws of England in 1765. Absolute rights were bestowed in the individual by the immutable laws of nature, in his opinion. Personal security, personal liberty, and property rights were distributed among these absolute rights. An individual's right to personal security entailed the legal and uninterrupted enjoyment of his or her life, limbs, body, health, and reputation.[15]

According to Mill: "The only part of the conduct of any one, for which he is amenable to society, is that which concerns others. In the part which merely concerns himself, his independence is, of right, absolute. Over himself, over his own body and mind, the individual is sovereign."[16]

James Madison, the architect of the American Constitution, contemplated the protection of the faculties of the citizen as a part of the inalienable property rights of human beings.

---

[14] Michael C. James, *A Comparative Analysis of the Right to Privacy in the United States, Canada and Europe*, 29:2, Connecticut Journal of International Law, *261* (Spring 2014),

[15] Justice K.S. Puttaswamy v. UOI, (2017) 10 SCC 1, Para 40

[16] JOHN STUART MILL, ON LIBERTY, 13, (Batoche Books 1859),

"In the former sense, a man's land, or merchandize, or money is called his property. In the latter sense, a man has property in his opinions and the free communication of them… He has an equal property interest in the free use of his faculties and free choice of the objects on which to employ them. In a word, as a man is said to have a right to his property, he may be equally said to have a property in his rights. Where an excess of power prevails, property of no sort is duly respected. No man is safe in his opinions, his person, his faculties or his possessions…Conscience is the most sacred of all property; other property depending in part on positive law, the exercise of that, being a natural and inalienable right. To guard a man's house as his castle, to pay public and enforce private debts with the most exact faith, can give no title to invade a man's conscience which is more sacred than his castle, or to withhold from it that debt of protection, for which the public faith is pledged, by the very nature and original conditions of the social pact."[17]

In the article 'The Right to Privacy', authors Samuel D. Warren and Louis D. Brandeis traced out the 'right to be let alone' which was synonymous to the right to privacy.[18] The authors state that, "The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury. The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality".

"Warren and Brandeis defined an already existing common law right as a stepping stone to the right to be let alone, such as the right to determine to what extents the thoughts, the sentiments and emotions of the individual shall be communicated to others. The principle of this right was the inviolate personality"[19]. The right to be let alone basically ensured protection against the unwanted disclosure of private facts, thoughts, emotions, etc.[20]

---

[17] James Madison, *Essay on Property*, in Gaillard Hunt ed., 6 The Writings of James Madison 101-103, (1906).
[18] Brandeis, *supra* note 3

[19] Bratman, *B. E.: Brandeis and Warren's The Right To Privacy and the Birth of the Right to Privacy,* 69 Tennessee Law Review 344 (2002)

[20] Prosser, W.: *Privacy, 48:3* California Law Review, 384 (1960)

2.3. RIGHT TO PRIVACY IN INTERNATIONAL LAW

The human rights movement reached a pinnacle when a deliberate effort was made to codify such intrinsic human rights. Human rights jurisprudence has gained more traction in local and international judicial forums with the establishment of the United Nations and the inclusion of human rights as a key issue of international law and politics. International and regional treaties have acknowledged the right to privacy in many jurisdictions. The significance of privacy in this respect is demonstrated by the fact that it occurs in almost every human rights-related treaty or dialogue.

The right to privacy in modern human rights jurisprudence emerges in 1948 in Article 12 of the **Universal Declaration of Human Rights** (UDHR) which states:

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[21]

This provision aims to establish a legal framework in the international order that requires states to guarantee physical and communication privacy. Furthermore, this role aims to cover a wide range of human interaction and behaviour. These aspects of dignity include the right to reputation and the privacy of one's family. Human rights law is widely acknowledged as having the goal of fostering human personality and protecting it from undue intervention. As a result, in attempting to attain the purpose of human rights law, privacy emerges as the central focus.

The **International Covenant on Civil and Political Rights (ICCPR), 1966** in Article 17 has reiterated the aforesaid position of privacy as contained in the UDHR as a right that merits protection of law by stating:

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

2. Everyone has the right to the protection of the law against such interference or attacks."[22]

Article 14 of the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families uses a similar notion in the context of migrant worker

[21] UN Peace, Dignity and Equality on a Healthy Planet, https://www.un.org/en/about-us/universal-declaration-of-human-rights, (last visited on 10/10/2021- 7:30 pm)

[22] United Nations Office of the High Commissioner, https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx, (last visited on 10/10/2021- 7:30 pm)

rights.[23] The right contained therein to protect migrant workers and their families from arbitrary interference with their family life and privacy. Article 16 of the Convention on the Rights of Child[24] and Article 22 of the Convention on the Rights of Persons with Disabilities[25] also specifically seek to establish protection of privacy of children and persons with disabilities.

On 30 June 2014, a report of UN High Commissioner for Human Rights stated on Privacy rights in digital age that: "there is universal recognition of the fundamental importance, and enduring relevance, of the right to privacy and of the need to ensure that it is safeguarded, in law and in practice". [26]

2.4. PRIVACY IN VARIOUS REGIONAL HUMAN RIGHTS CONVENTIONS

2.4.i. European Convention on Human Rights (ECHR) 1950

The European Convention on Human Rights (ECHR) establishes the foundation for an advanced privacy system in the world, as stated in Article 8[27]. In a democratic society, privacy is not viewed as an absolute right, and it is subject to certain limitations that are deemed appropriate. These exceptions must be applied in accordance with special legislation enacted

[23] International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, 1990- Article 14 No migrant worker or member of his or her family shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home, correspondence or other communications, or to unlawful attacks on his or her honour and reputation. Each migrant worker and member of his or her family shall have the right to the protection of the law against such interference or attacks.

[24] Convention on the Rights of Child, 1989, Article 16 (1.) No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.

[25] Convention on the Rights of Persons with Disabilities, 2007

Article 22- Respect for privacy

1. No person with disabilities, regardless of place of residence or living arrangements, shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence or other types of communication or to unlawful attacks on his or her honour and reputation. Persons with disabilities have the right to the protection of the law against such interference or attacks.

2. States Parties shall protect the privacy of personal, health and rehabilitation information of persons with disabilities on an equal basis with others.

[26] "The Right to privacy in the Digital age", Report of the Office of the United Nations High Commissioner for Human Rights (30 June 2014).

[27] 8. Right to Respect for Private and Family Life. –
1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

in this area. Authorities may not interrupt with this right unless it is "in accordance with law and is necessary in the interests of a democratic society, in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health and morals, or for the protection of the rights and freedoms of others" as stated in Article 8.

As a result, the requirements can only be avoided under very specific circumstances. Furthermore, the European Council Directive makes it mandatory for member states to legislate on the subject of privacy and data protection in accordance with the directive's provisions.[28]

2.4.ii. American Convention on Human Rights, 1969

American Convention on Human Rights[29] has made privacy a priority in its design.

"Article 11 states:

1. Everyone has the right to have his honour respected and his dignity recognized.
2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honour or reputation.
3. Everyone has the right to the protection of the law against such interference or attacks."

2.4.iii. African Charter of Human and People's Rights, 1981 (ACHPR)

The ACHPR does not explicitly set out the right to privacy, but Article 18 attaches particular importance to the State's duty to protect the family life.[30]

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

Article 10 of the Charter ensures right to privacy of children, "No child shall be subject to arbitrary or unlawful interference with his privacy, family, home or correspondence, or to the attacks upon his honour or reputation, provided that parents or legal guardians shall have the

[28] Directive 95/46/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046 (last visited on 6/10/2021, 10:30 pm)

[29] AMERICAN CONVENTION ON HUMAN RIGHTS "PACT OF SAN JOSE, COSTA RICA", 1967

[30] Article 18- 1. The family shall be the natural unit and basis of society. It shall be protected by the State which shall take care of its physical health and moral.

2. The State shall have the duty to assist the family which is the custodian or morals and traditional values recognized by the community.

3. The State shall ensure the elimination of every discrimination against women and also ensure the protection of the rights of the woman and the child as stipulated in international declarations and conventions.

4. The aged and the disabled shall also have the right to special measures of protection in keeping with their physical or moral needs.

right to exercise reasonable supervision over the conduct of their children. The child has the right to the protection of the law against such interference or attacks".[31]

2.8. RIGHT TO PRIVACY IN INDIA

The Indian Constitution does not specifically and expressly give any right to privacy. The right to privacy is not listed in the Constitution as a fundamental right. Right to privacy can traced in the Constitution from the expressions in Preamble[32] and provisions in the Part III[33] of the Constitution.

The various cases relating to the right to privacy and the judicial response to the same are discussed in detail in the following paragraphs.

1. **M.P. Sharma v. Satish Chandra**[34]

One of the earliest cases of Right to Privacy, the provisions of the Criminal Procedure Code providing for Search and Seizure was under challenge. The Supreme Court, declining the right to privacy, speaking through a three-judge Bench held:

> "When the Constitution makers have thought fit not to subject such regulation to constitutional limitations by recognition of a fundamental right to privacy, analogous to the [American] Fourth Amendment, we have no justification to import it, into a totally different fundamental right, by some process of strained construction."

The court had upheld the constitutionality of the impugned provision by stating that the state has a overriding power to conduct searches and seizures for security reasons.

2. **Kharak Singh v. State of U.P.**[35]

The petition before the Supreme Court challenges the constitutional validity of Chapter 22 (Regulations 236 and 237) of the U.P. Police Regulations and the powers conferred upon police

[31] African Charter on the Rights and Welfare of the Child, https://au.int/sites/default/files/treaties/36804-treaty-african_charter_on_rights_welfare_of_the_child.pdf, (last accessed 4/10/2021, 7:00 am)

[32] "liberty of thought, expression, belief, faith and worship" and "Fraternity assuring the dignity of the individual"

[33] Article 19 (1)(a)- Right to freedom of speech and expression', Article 19(1)(d)- Right to move freely throughout the territory of India'', Article 21- Right to life and Personal Liberty

[34] AIR 1954 SC 300

[35] AIR 1963 SC 1295

officials by its several provisions on the ground that they violate the right guaranteed to citizens by Articles 19(1)(d) and 21 of the Constitution.

The Court referred to J Frankfurter's observation in ***Wolf v. Colorado***[36] "The security of one's privacy against arbitrary intrusion by the police ... is basic to a free society. It is therefore implicit in 'the concept of ordered liberty' and as such enforceable against the States through the Due Process Clause. The knock at the door, whether by day or by night, as a prelude to a search, without authority of law but solely on the authority of the police, did not need the commentary of recent history to be condemned as inconsistent with the conception of human rights enshrined in the history and the basic constitutional documents of English-speaking peoples ... We have no hesitation in saying that were a State affirmatively to sanction such police incursion into privacy it would run counter to the guarantee of the Fourteenth Amendment." The Court observed. "It is manifest that by the knock at the door, or by the man being roused from his sleep, his locomotion is not impeded or prejudiced in any manner" and hence not violative of Article 19 (1)(d).[37] In our view clause (*b*) of Regulation 236 is plainly violative of Article 21 and as there is no "Law" on which the same could be justified it must be struck down as unconstitutional."[38] However, the majority of the Judges participating in the decision pointed out that the right to privacy is not a guaranteed right under our Constitution.

Justice Subba Rao in his dissent favoured in inferring the right to privacy from the expression 'personal liberty' in Art. 21. In the words of SUBBA RAO, J.: "Further, the right to personal liberty takes in not only a right to be free from restrictions placed on his movements, but also free from encroachments on his private life. It is true our constitution does not expressly declare a right to privacy as a Fundamental Right, but the said right is an essential ingredient of personal liberty. Every democratic country sanctifies domestic life.....".[39]

3. Govind v. State of M.P[40]

In Govind v. State of M.P., the Supreme Court undertook a more elaborate appraisal of the right to privacy. In Govind, the Court evaluated the constitutional legality of Regulations 855

[36] 338 US 25 (1949)

[37] Supra note 35 para 10

[38] Supra note 35 para 16

[39] Supra note 35 Para 28

[40] AIR 1975 SC 1378

and 856 of the M.P. Police Regulations, which provide for surveillance using a variety of methods. The regulation was upheld by the Court, who ruled that Art. 21 was not infringed because the regulation in question constituted a "process established by law," as defined by Art. 21. A limited Fundamental Right to Privacy "as an emanation" from Arts. 19(a), (d), and 21 was also recognised by the Court. The right to privacy is not, however, absolute; reasonable restrictions can be placed thereon in public interest under Art. 19(5). Thus, MATHEW, J., observed in Govind:

"The right to privacy in any event will necessarily have to go through a process of case-by-case development. Therefore, even assuming that the right to personal liberty, the right to move freely throughout the territory of India and the freedom of speech create an independent right of privacy as an emanation from them which one can characterise as a Fundamental Right, we do not think that the right is absolute." [41]

MATHEW, J., also observed :

"…Privacy and dignity claims deserve to be examined with care and to be denied only when an important countervailing interest is shown to be superior. If the Court does find that a claimed right is entitled to protection as a fundamental privacy right, a law infringing it must satisfy the compelling State interest test." [42]

4. **Malak Singh v. State of Punjab**[43]

The Supreme Court considered the validity of certain Surveillance under the Punjab Police Rules. The Bench acknowledged the necessity to strike a balance between the state's goal of preventing crime and preserving public safety and constitutional freedoms under Articles 21 and 19(1)(d), and decided that police monitoring could not infringe on an individual's personal liberty, dignity, or privacy. The Court also stated that, while crime prevention is a legitimate public interest, monitoring for this reason should also not be regarded "unlawful interference" with another person's life. Surveillance must be reasonably limited to allow full actualisation of an individual's fundamental rights. It was held that, '**S**urveillance may be intrusive and it may so seriously encroach on the privacy of a citizen as to infringe his fundamental right to

[41] AIR 1975 SC 1378, Para 28

[42] Id, Para 22

[43] (1981) 1 SCC 420

personal liberty guaranteed by Article 21 of the Constitution and the freedom of movement guaranteed by Article 19(1)(d). That cannot be permitted**.'**[44]

5. R. Rajagopal v State of Tamil Nadu[45]

In R. Rajagopal v State of Tamil Nadu, (popularly known as **Auto Shanker Case**) the question raised was concerning the freedom of press vis-à-vis the right to privacy of the citizens of the country. The Court summarised the following principles from the discussion in the judgments.

(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, child-bearing 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., 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.

(3) There is yet another exception to the rule in (1) above indeed, this is not an exception but an independent rule. In the case of public officials, it is obvious, right to privacy, or for that matter, the remedy of action for damages is simply not available with respect

[44]Id,, Para 6

[45] (1994) 6 SCC 632

to their acts and conduct relevant to the discharge of their official duties. This is so even where the publication is based upon facts and statements which are not true, unless the official establishes that the publication was made (by the defendant) with reckless disregard for truth. In such a case, it would be enough for the defendant (member of the press or media) to prove that he acted after a reasonable verification of the facts; it is not necessary for him to prove that what he has written is true. Of course, where the publication is proved to be false and actuated by malice or personal animosity, the defendant would have no defence and would be liable for damages. It is equally obvious that in matters not relevant to the discharge of his duties, the public official enjoys the same protection as any other citizen, as explained in (1) and (2) above. It needs no reiteration that judiciary, which is protected by the power to punish for contempt of court and Parliament and legislatures protected as their privileges are by Articles 105 and 104 respectively of the Constitution of India, represent exceptions to this rule.

(4) So far as the Government, local authority and other organs and institutions exercising governmental power are concerned, they cannot maintain a suit for damages for defaming them.

(5) Rules 3 and 4 do not, however, mean that Official Secrets Act, 1923, or any similar enactment or provision having the force of law does not bind the press or media.

(6) There is no law empowering the State or its officials to prohibit, or to impose a prior restraint upon the press/media." [46]

6. Peoples' Union for Civil Liberties v. Union of India[47]

The Supreme Court ruled in this case, known as the "telephone tapping case," that telephone tapping is a serious invasion of an individual's right to privacy, which is part of the right to "life and personal liberty" enshrined in Art. 21 of the Constitution, and that it should not be used by the government unless a public emergency or public safety interest requires it. It was held that "We have, therefore, no hesitation in holding that right to privacy is a part of the right to 'life' and 'personal liberty' enshrined under Article 21 of the Constitution. Once the facts in a given

[46] (1994) 6 SCC 632, Para 26

[47] (1997) 1 SCC 301

case constitute a right to privacy, Article 21 is attracted. The said right cannot be curtailed 'except according to procedure established by law"[48]

The People's Union of Civil Liberties—a non-profit organization—filed the petition as a public interest litigation under Article 32 of the Constitution, citing recent occurrences of telephone tapping. The petitioners have challenged the constitutional validity of Section 5 of the Indian Telegraph Act of 1885, which allows the Central or State Governments to use phone tapping in certain circumstances. The writ petition was submitted in response to the Central Bureau of Investigation's report on "Tapping of Politicians Phones" (CBD).

The Court established detailed guidelines to govern the State's discretion vested in it under Section 5 of the Indian Telegraph Act for the purposes of telephone tapping and interception of other messages, in order to protect the public interest from the government's arbitrary and unlawful exercise of power. The Court has expressed dissatisfaction with the State's failure to stipulate norms to prevent abuse of authority thus far. It is impossible to protect citizens' rights guaranteed by Arts. 19(1)(a) and 21 of the Constitution without a just and fair system for controlling the exercise of power under Section 5(2) of the Indian Telegraph Act. The "occurrence of any public emergency" or "in the interest of public safety" are the "sine qua non" for the application of the provisions under Section 5(2) of the Act; unless a public emergency has occurred or the interests of public safety demand, the authorities have no jurisdiction to exercise the powers conferred by the legislation.[49] The Court defined a public emergency as the occurrence of a sudden circumstance or state of affairs that affects the general public and necessitates quick action. The term 'public safety' refers to a state or situation in which the general population is in considerable danger or risk. The Court stated that if either of these two elements are not met, the Central Government, State Governments, or authorised officers cannot use telephone tapping, even if they believe it is necessary or expedient in the interests of the country's sovereignty and integrity.[50]

[48] Id, Para 17

[49] Id, Para 28

[50] Id,

7. District Registrar and Collector, Hyderabad & Anr v. Canara Bank[51]

In District Registrar and Collector, Hyderabad v Canara Bank, a Bench of two judges of the Apex Court considered the validity of the provisions of the Indian Stamp Act, 1899 (as amended by a special law in Andhra Pradesh). The Collector or "any person" authorised by the Collector was allowed to enter any premises to conduct an inspection of any records, registers, books, or documents in the custody of any public officer if the inspection resulted in the discovery of fraud or omission of any duty payable to the government under Section 73 of the Andhra Pradesh Stamps Act. The case's major issue concerned the privacy of a customer's records kept by a financial organisation like a bank. The Supreme Court ruled that the challenged provision was unconstitutional because it failed to meet the constitutional rationality requirements set forth in Articles 14, 19, and 21.The court held that any legislation intruding on the personal liberty of a citizen (in this case the privacy of a citizen's financial records) must, in order to be constitutional, satisfy the triple test laid down by the Supreme Court in ***Maneka Gandhi***[52], This triple test requires any law intruding on "personal liberty" under Article 21, to meet certain standards:

(i) must prescribe a procedure;

(ii) the procedure must withstand the test of one or more of the fundamental rights conferred under Article 19 which may be applicable in a given situation; and

(iii) it must also be liable to be tested with reference to Article 14.

The impugned provision was held to have failed this test. More crucially, the court determined that the concept of privacy applied to the individual rather than the location. Such a statement implied that it didn't matter whether the financial records were kept at a citizen's home or in a bank. As long as the financial records in question belonged to a person, the citizen's right to privacy would protect them.

8. Hinsa Virodhak Sangh vs Mirzapur Moti Kuresh Jamat & Ors[53]

The validity of resolution restricting the working of slaughterhouses during a short period of Jain festival was challenged. The Court observed that, 'What one eats is one's personal affair and it is a part of his right to privacy which is included in Art 21 of the Constitution'

[51] (2005) 1 SCC 496

[52] (1978) 1 SCC 248

[53] (2008) 5 SCC 33

9. State of Maharashtra vs. Bharat Shanti Lal Shah[54]

This case adjudicated the constitutional validity of the Maharashtra Control of Organised Crime Act, 1999 (MCOCA). Sec 13-16 of the Act providing for telephone tapping was challenged. The Court held that, 'The interception of conversation though constitutes an invasion of an individual right to privacy but the said right can be curtailed in accordance to procedure validly established by law. Thus what the Court is required to see is that the procedure itself must be fair, just and reasonable and non arbitrary, fanciful or oppressive." [55] The Court considered that these provisions create a 'procedure established by law' and have sufficient procedural safeguards embedded to save them from being unfair or arbitrary, since Section 16 provides punishments for an unauthorized user for information acquired by interception of wire, electronic or oral communication.[56] The Court upheld the validity of the impugned provisions.

10. Selvi v. State of Karnataka[57]

The case discusses legal issues surrounding the forcible administration of scientific procedures such as narcoanalysis, polygraph examination, and the Brain Electrical Activation Profile (BEAP) test for the aim of strengthening criminal investigation operations. It was held that such techniques violate the basic human right of an individual as the forcible administration of these techniques amounts to cruelty and is an intrusion of mental privacy. The bench ruled that involuntary administration of the impugned techniques violates the right against 'self-incrimination' under Art. 20 (3) of the Constitution.

11. Ram Jethmalani v. Union of India[58]

The Supreme Court was hearing a public interest case involving unaccounted funds and a request to create a Special Investigating Team to follow and investigate a money trail. It was observed that "An inquisitorial order, where citizens' fundamental right to privacy is breached

[54] (2008) 13 SCC 5

[55] Id, Para 60

[56] Id, Para 61

[57] AIR 2010 SC 1974

[58] (2011) 8 SCC 1.

by fellow citizens is destructive of social order. 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." [59] The Court held that "The revelation of details of bank accounts of individuals, without establishment of prima facie grounds to accuse them of wrong doing, would be a violation of their rights to privacy."[60]

12. Justice K.S. Puttaswamy v. Union of India[61]

In the nine-judge bench decision, the Supreme Court held Privacy as a Fundamental Right. However, it was also held that this right is not absolute but allowed for restriction where this was provided by law, corresponded to a legitimate aim of the State and was proportionate to the objective it sought to achieve. The Court overruled the decision in M.P. Sharma to the extent which holds that the right to privacy is not protected by the Constitution of India. The decision in Kharak Singh vs. State of UP to the degree that it holds that the right to privacy is not protected by the Constitution also stands over-ruled. The Court analysed various international and regional privacy laws, foreign decisions and concepts like informational privacy. Chandrachud J., writing for the plurality, holds that the right to privacy is not separate from the other liberties provided by Part III of the Constitution. It is seen as an inalienable natural right and an element of human dignity. "Chelameswar J. on the other hand, grounds the right to privacy, as comprising of three facets, namely repose (freedom from unwarranted stimuli), sanctuary (protection from intrusive observation) and intimate decision (autonomy to make personal life decisions)."[62] Nariman J. agrees with Gary Bostwick's conceptual understanding of privacy as encompassing "repose, sanctuary, and intimate decision". He expands the concept by classifying it into three categories: (1) that which involves invasion by the State into a person's physical body, (2) information privacy which captures unauthorised

[59] Id, Para 73

[60]Id, Para 77

[61] (2017) 10 SCC 1

[62] Bhandari, V., Kak, A., Parsheera, S., & Rahman, F., *An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict* (accessed on 25/08/2021, 5:20 pm) https://www.indrastra.com/2017/11/An-Analysis-of-Puttaswamy-Supreme-Court-s-Privacy-Verdict-003-11-2017-0004.html

uses of personal information, and (3) privacy of choice, or "individual autonomy over fundamental personal choices".

“On the other hand, Kaul J. acknowledges that privacy claims can be made against both state and non-state actors. In terms of the State, he raises worries about surveillance and profiling, while in terms of non-State actors, he underlines the role of technology, particularly in the form of ubiquitous data generation, collection, and usage in the digital economy. Kaul J. also discusses the implications of big data, namely its impact on an individual's activities and the chilling effect it may have on free speech and expression. As a result, he sees the necessity to protect some information from both public and private actors”.[63]

2.9. PRIVACY – A MULTIFACETED RIGHT

The right to privacy is a multidimensional right. Apart from the above-mentioned case laws that mostly deals with State Surveillance and interference a few more aspects are discussed herewith.

2.5.i. Bodily Privacy

Indian jurisprudence provides Indian jurisprudence provides immunity to medical records insofar as the right to privacy is concerned. However, this protection is qualified by the exception in the hands of courts, where non-disclosure may potentially endanger the lives of other beings.

In ***'X' v. Hospital 'Z'***[64], the Supreme Court considered the scope of a blood donor's right to privacy in his medical records. The respondent hospital in this case had disclosed the fact that the blood donor had been diagnosed as an HIV patient without the consent of the blood donor. The lady who was to have married the blood donor had broken off their engagement as a result of the hospital's announcement, condemning the donor to societal ostracism. While medical records are meant to be private, the Supreme Court determined that doctors and hospitals could make exceptions in particular circumstances when the non-disclosure of medical information could risk the lives of other people, in this case the wife's life. As a result, the purported intrusion was legalised on the basis of another person's right to health.

[63] Id

[64] (1998) 8 SCC 296

In ***Sharda v. Dharmpal***[65] the question for consideration was whether the Court could direct a person to undergo medical examination in the course of matrimonial proceedings. The Supreme Court held that there is no absolute right to privacy. In this case the conflicting rights were the right to seek divorce on grounds of unsoundness of mind of one party, which may require medical examination and the right to privacy of the other party. It was held that the Court could order medical examination if the applicant has a strong prima facie case.

In ***National Legal Services Authority v. Union of India***[66] upheld the 'right to life' of the transgenders. It was held that "Gender identity, therefore, lies at the core of one's personal identity, gender expression and presentation and, therefore, it will have to be protected under Article 19(1)(a) of the Constitution of India. A transgender's personality could be expressed by the transgender's behaviour and presentation. State cannot prohibit, restrict or interfere with a transgender's expression of such personality, which reflects that inherent personality. Often the State and its authorities either due to ignorance or otherwise fail to digest the innate character and identity of such persons. We, therefore, hold that values of privacy, self-identity, autonomy and personal integrity are fundamental rights guaranteed to members of the transgender community under Article 19(1)(a) of the Constitution of India and the State is bound to protect and recognise those rights."[67]

In Puttaswamy[68], it is held that sexual orientation is an essential attribute of privacy. It is observed that, "Discrimination against an individual on the basis of sexual orientation is deeply offensive to the dignity and self-worth of the individual. Equality demands that the sexual orientation of each individual in society must be protected on an even platform. The right to privacy and the protection of sexual orientation lie at the core of the fundamental rights guaranteed by Articles 14, 15 and 21 of the Constitution."[69]

2.5.ii. Women's Rights

In the sphere of women's rights, the right to privacy has been asserted. It is trite law that the right to privacy includes the right to reproductive autonomy, which includes, among other

[65] AIR 2003 SC 3450

[66] (2014) 5 SCC 478

[67] Id, Para 72

[68] (2017) 10 SCC 1

[69] Id,Para 127

things, the freedom to use a condom and the right to abort for women. While urging for harsh punishment for sexual violence, the Supreme Court ruled that rape is a grave infringement of right to privacy under Article 21. [70] In cases where women are witnesses or accused, they must be interviewed by female police officers at their residence while maintaining their privacy. This directive was given in response to a petition alleging police station torture and harassment of women. [71] In fact, the Supreme Court ruled that restitution of conjugal rights was a harsh remedy that denied the female the ability to control her own body and was unconstitutional since it violated her right to privacy.[72]

The question of the rights of prostitutes arose in ***State of Maharashtra v. Madhukar Narayan Mardikar***[73] where a police officer was terminated from his job after engaging in deviant behaviour with a woman. While the Maharashtra High Court decided that the woman's evidence could not be trusted, the Supreme Court ruled in favour of a prostitute's right to privacy, stating that an invasion of private cannot be justified on the basis of a woman's easy virtues. Every individual has the right to privacy and anonymity.

The court was dealing with issues emanating from a departmental investigation into a police officer suspected of invading the lady in question's home and ravishing her while in uniform. While pronouncing the judgment preserving a prostitute's right to privacy, K. Jagannatha Shetty and A.M. Ahmadi JJ of the Supreme Court held:

"Even a woman of easy virtue is entitled to privacy and no one can invade her privacy as and when he likes. So also it is not open to any and every person to violate her as and when she wishes. She is entitled to protect her person if there is an attempt to violate it against her wish. She is equally entitled to the protection of law. Therefore, merely because she is a woman of easy virtue, her evidence cannot be thrown overboard. At the most the officer called upon to evaluate her evidence would be required to administer caution unto himself before accepting her evidence."[74]

[70] State of Karnataka v. Krishnappa, (2000) 4 SCC 75

[71] State v. N.M.T. Joy Immaculate, (2004) 5 SCC 729

[72] Saroj Rani v. Sudarshan Kumar Chadha, (1984) 4 SCC 90

[73] (1991) 1 SCC 57

[74] (1991) 1 SCC 57, Para 8

In ***Roe v. Wade***(1973) ,[75] the US Supreme Court established that a woman's right to an abortion was protected by the right to privacy implicit in the Fourteenth Amendment. In ***Suchita Srivastava v. Chandigarh Administration,*** [76] the question was regarding the abortion of a pregnant raped mentally retarded orphan woman. It was observed that, "There is no doubt that a woman's right to make reproductive choices is also a dimension of 'personal liberty' as understood under Article 21 of the Constitution of India. 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".[77]

Hence, the definition of privacy has been broadened to include a variety of specific examples of abuse of women's rights. In the era of contemporary law, the right to privacy has a substantial impact on women's rights.

2.5.iii. Data or Informational Privacy

We live in the era of information. With the advent of internet, the world is at our fingertips. Every online transaction and every site we visit leaves and stores our digital footprints. These footprints contain information about the users and their interests. Individually, they might seem irrelevant. But in aggregation, it discloses the nature of personality, food habits, sexual orientation, health status, friendships, way of life and political affiliation.

In ***NASA v. Nelson***[78], informational privacy issues were addressed. NASA's background checks of contract personnel did not breach any constitutional privacy rights, the Court unanimously decided. It was held that, 'In light of the protection provided by the Privacy Act's nondisclosure requirement, and because the challenged portions of the forms consist of

[75] 410 U.S. 113 (1973)

[76] (2009) 9 SCC 1

[77] Id, Para 22

[78] 562 U.S. 134, 131 S. Ct. 746 (2011)

reasonable inquiries in an employment background check, we conclude that the Government's inquiries do not violate a constitutional right to informational privacy'.

In ***R v The Commissioner of Police of the Metropolis***[79] the extent of the police's power (under guidelines issued by the Association of Chief Police Officers- the ACPO guidelines) to indefinitely retain biometric data associated with individuals who are no more suspected of a criminal offence. The UK Supreme Court ruled unanimously that the police force's policy of holding DNA evidence in the absence of "extraordinary circumstances" was illegal and violated Article 8 of the European Convention on Human Rights.

Informational privacy has become more complicated in the information age. These problems stem from the nature of information. Information is non-rivalrous, invisible, and recombinant in three ways.[80] It is impossible for a judge to imagine all of the possible uses of information or their repercussions in this age of fast expanding technology:

"…The creation of new knowledge complicates data privacy law as it involves information the individual did not possess and could not disclose, knowingly or otherwise. In addition, as our state becomes an "information state" through increasing reliance on information – such that information is described as the "lifeblood that sustains political, social, and business decisions. It becomes impossible to conceptualize all of the possible uses of information and resulting harms. Such a situation poses a challenge for courts who are effectively asked to anticipate and remedy invisible, evolving harms."[81]

"An era of ubiquitous dataveillance, or the systematic monitoring of citizen's communications or actions through the use of information technology", as the current era has been appropriately described.[82] The tricky balance between the state's valid concerns and individual interest in privacy protection generates complicated issues, necessitating delicate balances to be established between both.

[79] [2011] UKSC 21

[80] Christina P. Moniodis, *Moving from Nixon to NASA: Privacy 's Second Strand- A Right to Informational Privacy,* 15:1Yale Journal of Law and Technology 154, (2012)

[81] Id

[82] Yvonne McDermott, *Conceptualizing the right to data protection in an era of Big Data*, Big Data and Society 1, (2017)

2.10. CONCLUSION

The right to privacy is a multifaceted right which is inherent in human beings. It is quintessential for a dignified human life. From the early periods where privacy was not even considered as a right to the present day where it is recognised as a fundamental right, society has advanced, so has its aspirations on rights. In India the right to privacy is implicit in various Articles of the Constitution like Art.19, 21, 25 read with Preamble. Though the right to privacy is accepted as a fundamental right is not an absolute one. Absolute right to privacy is however a threat to law and order and security and it is practically impossible as well. The State or non-state actors can intervene in a person's privacy only through lawful means for lawful purpose in a reasonable manner.

CHAPTER 3

DATA PRIVACY WITH SPECIAL REFERENCE TO THE RIGHT TO ERASURE AND RIGHT TO BE FORGOTTEN

"Although we feel unknown, ignored
As unrecorded blanks,
Take heart! Our vital selves are stored
In giant data banks,

Our childhoods and maturities,
Efficiently compiled,
Our Stocks and insecurities,
All permanently filed,

Our tastes and our proclivities,
In gross and in particular,
Our incomes, our activities
Both extra-and curricular.

And such will be our happy state
Until the day we die
When we'll be snatched up by the great
Computer in the Sky"[83]

3.1. INTRODUCTION

In the information age where we use digital tools for almost everything in our daily activities, little do we know about us creating eternal digital footprints. Daniel J Solove, in his book, 'The Digital Person'[84] explains how privacy is invaded and data is eternally stored in the information age. "The time will come, predicts one marketer, when we are well known for our inclinations, our predilections, our proclivities, and our wants. We will be classified, profiled, categorized,

[83] Felicia Lamport, "DEPRIVACY", Look Magazine, 1970.
[84] DANIEL J SOLOVE, THE DIGITAL PERSON, 26 (New York university Press, 2004).

and our every click will be watched. As we live more of our lives on the Internet, we are creating a permanent record of unparalleled pervasiveness and depth. Indeed, almost everything on the Internet is being archived. One company has even been systematically sweeping up all the data from the Internet and storing it in a vast electronic warehouse."[85]
Our online identities are reflected in our websites and social media posts. We're used to seeing material on the internet appear and vanish, creating the sense that it's only temporary. However, almost little is lost or forgotten when we delete or update material on the Internet. The quantity of information stored will only increase as our lives become continually digitised into the domain of cyberspace.[86]

3.2. DATA AND BIG DATA

Data are records of observations or actions, or patterns of symbols that represent values or actions seen. Instrument readings, x-ray or scanner images, voice recordings, family lineage charts, interview responses, hospital billing files, and a plethora of other outcomes of looking, asking, listening, measuring, recording, or analysing are just some of the possibilities.[87] Almost all data in research is now managed digitally, even if it necessitates transcription or translation from nondigital formats. Of course, this substantially helps computerised analysis. It also enables the transmission of data from one site to another with near-light speed and at a cheap cost, which can be either beneficial or problematic depending on how the data is managed and used. The term "information" refers to data that has been placed in an interpretive framework in order to establish meaning. Information and data are frequently used interchangeably. [88]

Data is defined in Sec 2(*11*) of the draft Data Protection Bill, 2019 as "data includes a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by humans or by automated means"[89]; and Sec 2 (*28*) defines "personal data"- "means data about or relating to a natural person who is directly

[85] Id

[86] Id

[87] WILLIAM W. LOWRANCE, PRIVACY, CONFIDENTIALITY AND HEALTH RESEARCH 7 (Cambridge University Press, 2012).

[88] Id

[89] Sec 2 (11) of the Draft Data Protection Bill, 2019.

or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling"[90]

As per Sec 2 (o) of the Information Technology Act 2000,data "means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;"[91]

Yvonne McDermott in her article "Conceptualizing the right to data protection in an era of Big Data"[92] states that, "Big Data is a notoriously difficult concept to find a commonly accepted definition for (Ward and Barker, 2013), but a number of key features of Big Data have been identified, including: the huge volume of data, the speed at which it is collected, the variety of data, its relational nature (allowing linkages to be made to other data sets), and potentially exhaustive scope (Kitchin, 2013: 262)."[93]

The definition given by International Business Machines Corporation is "Big Data is not about the data, any more than philosophy is about words. Big Data is about the value that can be extracted from the data or the meaning contained in the data. The term Big Data really means harvesting meaning from data that is coming in faster, from more sources, and in more varied formats than ever before. We should probably call it Big Meaning because Big Data is really about the value (meaning) in the data, rather than the data itself."[94]

The Internet of Things (IoT) refers to the embedment of sensors and mechanisms in common everyday objects such as refrigerators cars, especially autonomous vehicles, roads, pacemakers

[90] Sec 2 (28) of the Draft Data Protection Bill, 2019.

[91] Sec 2 (o) of the Information Technology Act 2000.

[92] McDermott, *supra* note 79

[93] McDermott, *supra* note 79

[94] J.Steven Perry, What is Big Data? More than Volume, Velocity and Variety...IBM Developer Blog (2017). https://developer.ibm.com/blogs/what-is-big-data-more-than-volume-velocity-and-variety/, (last accessed on 06/7/2021- 6:53 am.)

and watches that collect and store information, and that also allows the information to be transmitted to other objects or machines usually through Internet in a wireless manner. All this information collected is combined to make up what is loosely called "big data". [95]

In a report written to the White House,[96] IoT was defined as

"[A] term used to describe the ability of devices to communicate with each other using embedded sensors that are linked through wired and wireless networks. These devices could include your thermostat, your car, or a pill you swallow so the doctor can monitor the health of your digestive tract. These connected devices use the Internet to transmit, compile, and analyze data.".

The variety and sophistication of data sources and formats is growing. Just a few examples include the public web, social networking sites, mobile applications, federal, state, and local registers and databases, commercial datasets that accumulate individual information from a multitude of commercial transactions and public records, geospatial data, surveys, and conventional documents scanned into electronic form. [97]As more Internet-enabled devices and sensors have been available, the potential to collect data from physical goods such as detectors and radio-frequency identification (RFID) chips has expanded. Personal location data can be obtained using GPS devices, cell-tower triangulation, wireless network charting, and in-person payments.[98]

"Vast amounts of data are being created and collected everyday by the interactions of billions of people using computers, mobile phones and other electronic devices. Online or mobile financial transactions, social media traffic and global positioning system co-ordinates now generate over 2.5 quintillion bytes of big data every day." [99]

Big data provides knowledge about individuals that was just not possible to know in past generations when enormous datasets are collected and integrated. It discloses who a person

---

[95] HANNAH YEEFEN LIM, DATA PROTECTION IN THE PRACTICAL CONTEXT, 12 (Academy Publishing, 2017)

[96] *Big Data: Seizing Opportunities and Preserving Values,* Executive Office of the President, May 2014, https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf accessed on 10/07/2021, 14:30 pm.

[97] Id

[98] Id

[99] Lim, *supra* note 95

speaks with, what is said to them, where they go, where they work, who they work for, who their kith and kin are, where they eat, what they eat, what they buy, and so on. It reveals preferences, hobbies, financial status, employment status, and even criminal backgrounds. Complete profiles can be put together.[100]

3.3. DIGITAL AGE AND PRIVACY

"In network societies, the individual has emerged simultaneously as a data subject, and as a quantified self. The quantified self is contingent upon big data harvesting mechanisms that embed the individual not only as willing subjects to technologies of measurement and computing, but also participating in processes **of** quantification, becoming agents to the regimes of technology that operate upon the body. The data subject is closely related to the quantified self but specifically refers to the ways in which the individual finds expression, identity, subjectivity, and modes of negotiation with the networked technologies that operationalise the domains **of** life, labour, and language."[101]

The technology has made the world remain interconnected. Technology is now, an indispensable part of our daily activities. Our shopping habits have now changed to online purchases from visiting our neighbouring shops for groceries, we book flight or bus or hotel tickets online instead of delegating it to a travel agent, we buy medicines online, the E-books have opened a vast area of knowledge and we do online banking transactions which might come with 'offers' or 'cashbacks' apart from saving our time. Internet is now used for communication, purchasing of goods and services, business and what not. For every doubt that pops in our head 'google' provides answer within seconds.

The use of internet is shown to have increased since March 2020 after the outbreak of Covid 19 virus and the nationwide lockdown hitherto. The past year has seen a drastic change from traditional schooling where kids could go the school in person to e-schooling where kids are attending online classes. This has made devices like smartphone, laptop or tablet available to kids in order to effectuate their online classes. The meetings and conferences that required physical presence of speakers and participants have now shifted online, with apps like zoom,

[100] Lim, *supra* note 95 at 16

[101] Nishant Shah, *Identity and Identification: The Individual in the Time of Networked Governance*, 11 Socio-LEGAL REV. 22 (2015).

google meet etc. The governments across the world started using digital tools for covid tracking and monitoring.

With all the benefits that internet provides, its impact over a user's privacy is often left unnoticed. Every site we visit, every transaction we make, leaves electronic tracks, most often without our knowledge. These electronic tracks contain information which could provide knowledge about the user. Though these information silos individually might seem unnecessary. But in aggregate, they disclose the nature of the personality, food habits, language, health, hobbies, sexual preferences, way of dress, social and family networks, political affiliation and religious beliefs.[102]

Popular websites install cookie files by the user's browser. Cookies can be used to tag browsers with unique identifiers, allowing them to quickly recognise users and safeguard information about their online activities. User profiles are created using information, particularly a user's surfing history. Algorithms allow for the building of user profiles on the internet. Reading of user e-mails is mainly owing to automated content analysis of e-mails. A person's interests can be deduced from an e-mail, and appropriate adverts can be targeted to that user on the window's site. The books that a person buys on the internet leave a trail for targeted advertising in the same category. Whether a flight ticket was purchased in economy or business class reveals important information about an individual's work status and economic output. Taxi journeys to shopping centres that are booked online generate a profile of customer preferences. A lady who buys pregnancy-related medications on the internet will be bombarded with adverts for baby supplies. Electronic monitoring of people's lives is commonplace.[103]

The United States Supreme Court, in ***Whalen v. Roe***,[104] signalled its awareness of the privacy implications of information technology, stating:
"We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of the criminal laws all

[102] DANIEL J SOLOVE, UNDERSTANDING PRIVACY, 117 (Harvard University Press. 2008)

[103] Justice K.S.Puttaswamy v. Union of India, (2017) 10 SCC 1, 248

[104] 429 U.S. 589 (1977).

require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed."

Daniel Solove explains how privacy can be endangered by combining "relatively innocuous bits of information" as the combination paints "a rather detailed portrait of our personalities and behavior."[105] Solove calls this problem "aggregation" and "notes that businesses and government often aggregate a variety of information fragments, including pieces of information we would not view as private in isolation, to paint such a portrait."[106]
He explains, "As law professor Julie Cohen notes, [a] comprehensive collection of data about an individual is vastly more than the sum of its parts. I refer to this phenomenon as the "aggregation effect." Similar to a Seurat painting, where a multitude of dots juxtaposed together form a picture, bits of information when aggregated paint a portrait of a person. In the Information Age, personal data is being combined to create a digital biography about us. Information that appears innocuous can sometimes be the missing link, the critical detail in one's digital biography, or the key necessary to unlock other stores of personal information. As legal scholar Stan Karas points out, the products we consume are expressive of our identities." [107]

Christian P. moniodis, in her Article[108] states the peculiar character of information which makes it difficult to detect privacy violations. "The complexity of informational privacy is inherent in the nature of information itself: it is nonrivalrous, invisible and recombinant. These traits effectively blind judges to the harms at stake in data privacy cases. Firstly, information is a nonrival good in that there can be simultaneous users of the good; that is, one person's use of a piece of information does not make it less available to another. Moreover, data privacy invasions are difficult to detect because they can be invisible. Information can be accessed, stored, and disseminated without notice. The ability of information to travel at the speed of light enhances the invisibility of data access--that is, information collection can be the swiftest theft of all. Consequently, together, the invisible and nonrivalrous consumption of information allows for massive privacy invasions without any obvious harm to the invaded individuals.

[105] Solove, *supra* note 102 at 118

[106] Id

[107] Id

[108] Moniodis, *supra* note 80 at 161

Furthermore, information is recombinant: that is, data output can be used as an input to generate more data output, and so forth. For instance, through a developing application known as Knowledge Discovery and Data Mining processes, data can be combined to "create facts" about an individual; in particular, the likelihood that an individual will engage in a certain type of behavior. The creation of new knowledge complicates data privacy law as it involves information the individual did not possess and could not disclose, knowingly or otherwise. In addition, as our state becomes an "information state" through increasing reliance on information-such that information is described as the "lifeblood that sustains political, social, and business decisions" -it becomes impossible to conceptualize all of the possible uses of information and resulting harms. Such a situation poses a challenge for courts whom are effectively asked to anticipate and remedy invisible, evolving harms."

Changes in technology have made it easier to get pictures that were previously available to the public but were difficult to obtain. As a result of covert "soft surveillance," new technologies that extend the senses have made new types of data available. The fact that such surveillance allows for the collecting of personal data without the subject's consent or awareness creates opportunities for abuse. Changes in business models, which are increasingly focused on the concept of greater customization of services and goods, a process that necessitates the collection of vast amounts of personal data in order to carry out the necessary customization.[109]

3.3.i. Potential harms of Personal Data Collection

The potential harms of personal data collection are discussed by Moira Paterson & Maeve McDonagh[110].

"Big Personal Data is harmful to privacy because it removes the ability of individuals to exercise control over their own individual data, thereby undermining their autonomy (ie 'living and ordering a life of one's own choosing'). The concept of autonomy is central to liberal theory. Individual autonomy has been described by Christman as 'an idea that is generally understood to refer to the capacity to be one's own person, to live one's life according to reasons and motives that are taken as one's own and not the product of manipulative or distorting external forces'. Except to the extent that it is based exclusively on analysis of data collected and used

[109] Lim, *supra* note 95 at 13

[110] Moira Paterson & Maeve McDonagh, *Data Protection in an Era of Big Data: The Challenges Posed by Big Personal Data*, 44 Monash University Law Review 1 (2018).

with the informed consent of the individuals concerned, Big Personal Data undermines the autonomy of data subjects in the processing of their data; it also facilitates activities and actions that further undermine autonomy by subjecting their decision-making to manipulation."
It undermines human dignity by ignoring information subjects' choices about how their personal data is utilised, as well as their sentiments about how their data is processed and used. It diminishes human dignity by treating people as analytical objects and facilitates decision-making, further objectifying them.

The personal data aggregates can help in understanding people's behaviour, weaknesses etc and can be used to manipulate them. One example relates to its use in political campaigning, typified by allegations concerning the use of analytics to influence the outcome of the Brexit referendum and US presidential elections in 2016. Cathy O'Neil[111] argues that data profiling exercises are expanding in the world of politics. Political campaigns build scoring systems on potential voters---the likelihood of voting for a given party, stance on a given issue, and the extent to which one is persuadable on that issue. The asymmetric information is used by politicians to manipulate ones vote or donation.[112]

In the United States, for example, WalMart uses 'sales, pricing, and economic data, combined with demographic and weather data, to fine-tune merchandising ... and anticipate appropriate timing of store sales'.[113] "Decision-making based on Big Personal Data also exposes individuals and groups to differential treatment (for example, price discrimination based on differential discounts). This involves discrimination in the sense that it allows decisionmakers to draw fine-grained distinctions between individuals which are then used as a basis for differential treatment. While such practices are commonplace in some sectors, for example, the insurance sector, Big Personal Data permits their more widespread use in relation to information which has not previously been available. This raises important questions as to whether there are 'specific differences' additional to those currently protected by anti-discrimination laws which should not be ignored."[114]

[111] Cathy O Neil, *Big Data Algorithms are Manipulating Us*, WIRED, (accessed on 29-06-2021- 10:31 am) all-https://www.wired.com/2016/10/big-data-algorithms-manipulating-us/-
[112] Id
[113] Paterson & McDonagh, *supra* note 110
[114] Id

Corporations today are anxious for any customer data they can get their hands on, and their drive for knowledge is far from democratic. The information gathered goes beyond consumer perceptions of the product to include characteristics about the consumers themselves, such as lifestyle details and even a comprehensive psychological profile.

3.3.ii. Data Collection by State

With the 9/11 terrorist attack in the US, there was huge hue and cry for national security measures. It could be considered as a major contributory for the banalization of State surveillance for the security and safety of the Nations, across the world. The revelations by Edward Snowden in 2013 made it clear that the US National Security Agency had been inspecting the phone calls of its citizens.

Richard A Posner in his article 'Privacy, Surveillance and Law'[115] explains how data surveillance by the State could be helpful in maintaining national security. He says, if the profiles of the individuals are digitized, pooled and searched electronically, it would reveal the links and interactions among individuals.[116] The intelligence officials would get access to information having vast utility for identifying and tracking members of terrorist cells, their network and financial sources. He observes;

"Privacy is the terrorist's best friend, and the terrorist's privacy has been enhanced by the same technological developments that have both made data mining feasible and elicited vast quantities of personal information from innocents: the internet, with its anonymity, and the secure encryption of digitized data which, when combined with that anonymity, make the internet a powerful tool of conspiracy. The government has a compelling need to exploit digitization in defense of national security."[117]

Justice William O. Douglas, writing for the dissent in ***Osborn v. United States***,[118] noted:

"The time may come when no one can be sure whether his words are being recorded for use at some future time; when everyone will fear that his most secret thoughts are no longer his own, but belong to the Government; when the most confidential and intimate conversations are always open to eager, prying ears. When that time comes, privacy, and with it liberty, will be

[115] Richard A. Posner, *Privacy, Surveillance, and Law, 75* University of Chicago Law Review 245 (2008)

[116] Id, at 250

[117] Id, at 251

[118] 385 U.S. 323 (1966)

gone. If a man's privacy can be invaded at will, who can say he is free? If his every word is taken down and evaluated, or if he is afraid every word may be, who can say he enjoys freedom of speech? If his every association is known and recorded, if the conversations with his associates are purloined, who can say he enjoys freedom of association? When such conditions obtain, our citizens will be afraid to utter any but the safest and most orthodox thoughts; afraid to associate with any but the most acceptable people. Freedom as the Constitution envisages it will have vanished."[119]

Apart from national security, the State has other reasons for the collection and storage of data. For the purpose of administration including proper distribution of resources, crime management and allocation of funds require the collection of data. The analysis of these data could enforce the legitimate claims and prevent siphoning away of resources by others. In a welfare State, collection, storage and analysis of data is inevitable for the purpose of its functioning.

3.3.iii. Dataveillance

The concept of 'dataveillance' and its impact is discussed in detail by Daniel J.Solove in his book 'The Digital Person'.[120]

"As legal scholar Jerry Kang observes: [D]ata collection in cyberspace produces data that are detailed, computer-processable, indexed to the individual, and permanent. Combine this with the fact that cyberspace makes data collection and analysis exponentially cheaper than in real space, and we have what Roger Clarke has identified as the genuine threat of "dataveillance."

"Dataveillance, as information technology expert Roger Clarke defines it, refers to the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons. According to political scientist Colin Bennet, "[t]he term *dataveillance* has been coined to describe the surveillance practices that the massive collection and storage of vast quantities of personal data have facilitated." Dataveillance is thus a new form of surveillance, a method of watching not through the eye or the camera, but by collecting facts and data. Kang argues that surveillance is an attack on human dignity, interfering with free choice because it "leads to self-censorship. Likewise, Paul Schwartz claims that data collection "creates a potential for suppressing a capacity for free choice: the

[119] 385 U.S. 323, 353-54 (1966) (Douglas, J., dissenting).

[120] Posner, supra note 112 at 245.

more that is known about an individual, the easier it is to force his obedience." According to this view, the problem with databases is that they are a form of surveillance that curtails individual freedom."[121]

The modern version of Jeremy Bentham's 'panopticon'- a circular prison with cells arranged around a central wall from which the prisoners could be observed without their knowledge, is dataveillance. [122]

George Orwell's *1984* warned that "Big Brother Is Watching You." Orwell wrote about television cameras and microphones as the modern devices of surveillance. The digital computer, however, of which Orwell was ignorant, is a far more effective surveillance device- both government and the private sector can use it for precisely this purpose.[123] Adam De Moore[124] states video monitoring, global positioning systems, biometric technologies, along with data surveillance may provide law enforcement officials monitoring tools without unduly burdening those being watched.

In *United States v. Jones*[125], Justice Sonia Sotomayor observes that the novel methods of surveillance do not need physical search or intrusion. It was observed that "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. Disclosed in [GPS] data… will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on… The Government can store such records and efficiently mine them for information years into the future… And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: "limited police resources and community hostility…". Installing a

[121] Solove, supra note 83 at 46

[122] NEIL RICHARDS, INTELLECTUAL PRIVACY-RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE, 104 (Oxford University Press, 2015)

[123] George B. Trubow, *Protecting Informational Privacy in the Information Society*, 10 N. ILL. U. L. REV. 521 (1990).

[124] Adam D. Moore, *Toward Informational Privacy Rights*, 44 San DIEGO L. REV. 809 (2007).

[125] 565 US 400 (2012)

Global Positioning System (GPS) tracking device on a vehicle and utilising it to monitor the vehicle's movements, was unanimously decided to be a search under the Fourth Amendment.

3.3.iv. Covid Tracing Apps and Privacy

In an interesting development, the High Court of Kerala was approached in a writ petition against the Kerala Government regarding a government contract with a private US company called Sprinklr regarding collection and processing of Covid-19 data. "Life and data confidentiality is more or less equal in our eyes," remarked the Kerala High Court in its order[126]. In its interim order, the Honourable High Court of Kerala directed the anonymization of data before transferring it to third parties so that the privacy of the data subjects can be protected.

3.6. DATA PRIVACY

In the article Privacy in the Digital Age, the authors argue that 'For an individual, digital privacy is about the ability to shape one's own on- line identity and decide when, how and where to share parts of that identity with people, companies or other selected entities. The freedom to create an identity online is the essence of conceptual privacy; in practice, it lies in the ability to develop and curate a digital portrait that reflects personal preferences.'[127]

Mark Burdon in his Book 'Digital Data Collection and Information Privacy Law'[128] states about Information Privacy Law, "Information privacy law provides a range of life-cycle protections that begin at the point of data collection and end with destruction or de-identification of no-longer-required data. In the interim, data collection organisations have a range of obligations to fulfil: the individual should be notified about the purposes of collection so that they can meaningfully consent to subsequent uses. Personal information can generally only be used for a defined purpose about which the individual is adequately informed. Individuals have a range of interaction mechanisms that seek to ensure the maintenance of control by giving them the ability to affirm the accuracy and currency of collected personal information. Personal information, once collected and stored, must be kept secure."

[126] W.P (C) Temp No.84, 129, 148, 163 of 2020

[127] Nuala O'Connor, Alethea Lange and Ali Lange, *Privacy in the Digital Age*, Great Decisions, 19, 17-28(2015),

[128] MARK BURDON, DIGITAL DATA COLLECTION AND INFORMATION PRIVACY LAW 2 (Cambridge University Press, 2020)

When obtaining personal data, the entity collecting it is expected to follow fair information practises. Fair information practises are standards of conduct that must be observed by organisations that collect and use personal data in order to ensure that the data is effectively secured. These practises include giving individuals with personal information notice and awareness that their information is being collected, giving people choices on how their personal information is used, enables individuals to review and contest information recorded about them in a timely and cost-effective way, and taking steps to determine that the data gathered about them is accurate.[129]

"In reflecting on what guidelines can best protect online informational privacy in a commerce-related setting, the US Federal Trade Commission has argued for federal legislation mandating the application to commercial Web sites of the four principles of fair information practice: *notice, choice, access* and *security*, principles that were first developed out of concern for the impact on individual privacy of the rapid growth of computerized databases among a host of federal government agencies. When applied to an online environment, the principle of *notice* requires that commercial Web sites not only let their visitors know what personal information is being collected about them but also how this information is collected, whether or not it is distributed to third parties, and whether or not other parties (such as DoubleClick) are permitted to gather information at these sites. Adequate *choice* involves letting online consumers decide if the information they knowingly provide to a Web site for a particular purpose can then be used by that Web site for other reasons. The principle of *access* gives consumers the ability to examine the data collected about them by a particular site and make corrections if necessary, while *security* means that Web sites need to protect the personal information they collect from falling into the hands of unauthorized others." [130]

3.7. RIGHT TO BE FORGOTTEN

In the book 'Delete'[131] starts with the story of one Ms. Stacy Snyder. Ms. Stacy was a 25-year-old single mother who had all the credits to be appointed as a teacher. The university officials

[129] JAMES WALDO, HERBERT S. LIN, LYNETTE I. MILLETT, ENGAGING PRIVACY AND INFORMATION IN A DIGITAL AGE 48 (The Academies Press, 2007)

[130] Diane P. Michelfelder, *The moral value of informational privacy in cyberspace*, 3 Ethics and Information Technology 129–135, (2001)

[131] VIKTOR MAYER SCHONBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE, (Princeton University Press, 2009)

summoned her to inform that she is denied the certificate as her behaviour was 'unbecoming' a teacher. The reason for the university's decision was shocking. A photo of her in costume wearing a pirate's hat and drinking from a plastic cup with the caption 'drunken pirate' was uploaded by her in the platform 'MySpace' was the culprit. After this incident she tried to remove the photo. However, the damage was already done. The Internet remembered what Stacy wanted to erase, remove and forget.

The nature and quantity of information available about individuals has evolved dramatically since the Internet's inception. Newspaper reporting and official or government records are no longer the only sources of personal information. Every page or event we like, like, or share, as well as our use of social media, Twitter micro-discussions, images and videos uploaded by us or others tagging us, and every page or event we like, favourite, or share, all contribute to our digital footprint. When you factor in information made not by us but about us by both public and private agencies that save data about individuals in databases, our digital shadows begin to significantly outnumber the data we create. It is abundantly evident that we live in a Big Data environment, where algorithms track our digital selves' repetitive behaviour. In this context, a system that allows some of this digital shadow to be purged makes logical.[132]

3.7.i. Google Spain Case[133]

One Mr. Gonsalez filed a request before the Spanish Data Protection Agency seeking removal of search results that appear on searching his name on google. The results were newspaper pages of some auction to repay his debts that happened decades ago. Mr. Gonzalez argued that the passage of time and the fact that the procedures in question were concluded rendered all references to them obsolete. The Spanish Data Protection Agency dropped the case against the publication, while the complaint against Google was upheld. The data was ordered to be removed from Google's index and prevented from being accessed again. Google filed a petition to reverse the decision. A number of enquiries were subsequently forwarded to the European Union's Court of Justice by the Spanish court. [134]

[132] Amber Sinha, *Right to be Forgotten – A Tale of two Judgments*, Centre for Internet Society, (last accessed on 18/04/2021) https://cis-india.org/internet-governance/blog/right-to-be-forgotten-a-tale-of-two-judgments

[133] **Google Spain SL, Google Inc v. Agencia Espanola de Proteccion de Datos es Mario Costeja Gonzalez ECLI:EU:C:2014:317 [Case Number C-131/12]**

[134] Mike Wagner & Yun Li-Reilly, The Right to be Forgotten, 72:6 The Advocate, Nov. 2014

By allowing any Internet user to get a structured overview of information relating to that individual on the Internet by searching for that individual's name, the court ruled that Google "processed" personal data. Furthermore, this data connected to aspects of Mr. Gonzalez's personal life that could not have been linked or discovered without the use of a search engine. According to the court, search engines aggravate the invasion of a person's privacy by making information "ubiquitous." The "simple economic interest" of the search engine operator did not justify the potentially highly serious interferences with an individual's rights. Most importantly, the court found that even legally permissible data processing can become incompatible with the law over time. This will be the case if the data are "inadequate, irrelevant, or excessive in reference to the purposes of the processing... not kept up to date, or... maintained for longer than is required" in light of the reasons for which they were gathered or processed. The court concluded that, in most situations, the European Charter's privacy rights should take precedence over not just the search engine operator's corporate interests, but also the interests of the general public. [135]

The right to be forgotten "reflects the claim of an individual to have certain data deleted so that third persons can no longer trace them."[136] It has been defined as "the right to silence on past events in life that are no longer occurring."[137] The right to be forgotten allows individuals to have personal information, videos, or images removed from specific online records so that they are no longer appear in search engines. The right to be forgotten differs from the right to privacy in the aspect that the right to privacy refers to information that is not publicly available, whereas the right to be forgotten entails removal of information that was publicly available till the time of removal and preventing third parties from accessing it.[138]

In theory, the right to be forgotten solves a critical issue in the digital age: it is extremely difficult to erase your online history now that every photo, status update, and tweet is stored in the cloud for all time. However, Europeans and Americans take quite different approaches to

[135] Id

[136] Weber, Rolf H. *"The right to be forgotten." More than a Pandora's Box*, 2 Journal of Intellectual Property, Information Technology and E-commerce,120-130 (2011)

[137] Pino, G. (2000). "The right to personal identity in Italian private law: Constitutional interpretation and judge-made rights". In: M. Van Hoecke; F. Ost (eds.). The harmonization of private law in Europe (pp. 225-237). Oxford: Hart Publishing. p. 237.

[138] *Kashmir Hill, (July 6, 2011). "Revenge Porn With A Facebook Twist". Forbes.* (last visited on 22/08/2021, 10:30 am) https://www.forbes.com/sites/kashmirhill/2011/07/06/revenge-porn-with-a-facebook-twist/?sh=4393773b1d2e

the problem. The intellectual roots of the right to be forgotten in Europe can be found in French law, which recognises le droit I l'oubli—or the "right of oblivion"—a right that allows a convicted criminal who has served his time and been rehabilitated to object to the publication of the facts of his conviction and incarceration for the purpose of social reintegration.[139]

A disturbing historical example of the misuse of data collected is described in 'Delete; The virtue of forgetting in Digital Age'[140] . In the 1930 s the Dutch government created a population registry collecting names, address, date of birth, religion and other personal information of its citizens. The registry was created for the purpose of facilitating administration and policy making. However, when the Nazis invaded the Netherlands, they took possession of the registry. It was misused for identifying and locating Jews and persecuting them ruthlessly. The registry made it easy for the Nazis to identify the Jews owing to which the highest percentage of persecution was marked in Netherlands. The author states that the citizens trusted their government and had no idea about what the future has for us, he warns that this could happen to any country.

3.7.ii. Right to be forgotten in across the world

- **EU**

The 1995 Data Protection Directive of the European Union includes the principle underpinning the right to be forgotten. Article 12 of the Directive provides that a person can ask for the data to be rectified, erased or blocked once that data is no longer necessary. Google Spain case has also upheld the right to be forgotten in the EU. Article 17[141] of EU Regulation 2016 provides

---

[139] Jeffrey Rosen, *The Right to be Forgotten*, Symposium Issue, 64 STANFORD LAW REVIEW ONLINE 88, (Feb. 13, 2012,) https://review.law.stanford.edu/wp-content/uploads/sites/3/2012/02/64-SLRO-88.pdf (last visited on 22/08/2021, 2:00 pm)

[140] VIKTOR MAYER SCHONBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE, 85 (Princeton University Press, 2009)

141 Art. 17 GDPR- Right to erasure ('right to be forgotten')

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
    1. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
    2. the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

for right to be forgotten where the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed, the personal data have been unlawfully processed or the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject.

- **US**

In June **2015,** about one year after the *Costeja* decision, Google announced a big change to its user policy on removing links from Google searches. The change applied to people in the United States and elsewhere-specifically to victims of revenge porn. Revenge porn occurs when a person publishes nude photos of an ex-lover to exact revenge. Female victims of revenge porn have reported experiencing harrowing ordeals from having nude photos of them follow them in Google searches of their names. The change in policy marked an important shift in Google's approach. Google has been relatively unreceptive to any privacy requests by users to change search results, except for a limited class of personal information: signatures, bank accounts, and other sensitive ID information. In those limited circumstances, Google will allow a delisting of a link from search results. Google has also allowed deranking of search results containing mug shots of people, as well as sites with repeated notices of copyright infringement.[142] This shows the increase enforcement of the right to be forgotten in the US.

3.7.iii. Right to be forgotten in India

The right to be forgotten is covered by the right to privacy. The right to be forgotten presents a legal quandary in India. Despite the importance of such a right, India's Information Technology (IT) Act 2000 (as revised in 2008) and the IT Rules, 2011 have no such provision. There has been contradictory views taken by various High Courts.

3. the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

4. the personal data have been unlawfully processed;

5. the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

6. the personal data have been collected in relation to the offer of information society services referred to in Article 8(1)

[142] Edward Lee, "The Right to be Forgotten v. Free Speech" Journal of Law and Policy for the Information Society, 103 (2015)

- Dharamraj Bhanushankar Dave v. State of Gujarat & Ors.[143]

The Gujarat High Court was approached against the publication of a judgement by Indian Kanoon, which was a "non-reportable judgement" and was presented by Google in its search results. According to the Petitioner, such an act was in violation of Article 21. The Petitioner claimed that Google and Indian Kanoon lacked the legal authority to broadcast a nonreportable judgement, which had harmed his personal and professional life. He further claimed that because of the disclosure, the ruling was widely available on the internet, which went against the Court's categorization.

The Court observed that "*The judgment in appeal is part of the proceedings and the said judgment is pronounced by this Court and therefore, merely publishing on the website would not amount to same being reported as the word "reportable" used for judgment is in relation to it being reported in law reporter."*[144]

The Court opined that there was no legal basis for ordering such removal, and the presence of the judgement on the Internet did not infringe on the petitioner's Article 21 rights.

- Sri Vasunathan v The Registrar General[145]

The Petitioner, a father filed a Writ Petition in the Karnataka High Court seeking orders to block his daughter's name in an earlier order passed by the Court, as his daughter feared the consequences of having her name associated with this earlier matter, and if a name-wise search was conducted by any person through any internet service provider such as Google or Yahoo, this order could be reflected in the results. The Petitioners' daughter was concerned that this would harm her marriage, as well as her reputation and goodwill in society.

The Court Observed that "This would be in line with the trend in western countries of the 'right to be forgotten' in sensitive cases involving women in general and highly sensitive cases involving rape or affecting the modesty and reputation of the person concerned."

[143] 2017 SCC Online Guj 2493

[144]Id, Para 7

[145] 2017 SCC Online Kar 424

The Court instructed its registry to make every effort to guarantee that any public-domain internet search does not return the petitioner's daughter's name in the case-title or the content of the order in the criminal petition.

- Judgement of the Kerala High Court in the Civil Writ Petition No. 9478 of 2016

In an order dated February 23, 2017, the Kerala High Court declared in favour of the Right to be Forgotten. In this case, the petitioner filed a writ petition before the Kerala High Court to safeguard their right to privacy under Article 21 of the Constitution. The petitioner requested that the Court issue orders ensuring that their identity would be protected and that any items identifying their name on Indian Kanoon, Yahoo, and Google would be removed or concealed appropriately. The Court issued an interim order in favour of the petitioner, directing Indian Kanoon to remove the petitioner's name from orders posted on its website until further orders were issued, due to the seriousness of the issue and Indian Kanoon's failure to appear before the Court despite being served with a notice.

- Zulfiqar Ahman Khan v. M/s Quintillion[146]

The petitioner approached the Delhi High Court in removing the news the defendants had published about him in the wake of #metoo campaign. Recognizing the Plaintiff's right to privacy, which includes the "Right to be Forgotten" and "Right to be Left Alone," the Court ordered that “any republication of the content of the originally impugned articles dated 12th October 2018 and 31st October 2018, or any extracts/ or excerpts thereof, as also modified versions thereof, on any print or digital/electronic platform shall stand restrained during the pendency of the present suit”[147]

- Subhranshu Rout v. State of Orissa[148]

The Orissa High Court was dealing with the bail application of the accused who raped a woman and uploaded the video of the same on social networking sites. The Court declining his bail observed the Right to be forgotten and held, “However, allowing such objectionable photos and videos to remain on a social media platform, without the consent of a woman, is a direct

[146] 2019 SCC Online Del 8494

[147] Id, Para 9

[148] 2020 SCC Online Ori 878

affront on a woman's modesty and, more importantly, her right to privacy. In such cases, either the victim herself or the prosecution may, if so advised, seek appropriate orders to protect the victim's fundamental right to privacy, by seeking appropriate orders to have such offensive posts erased from the public platform, irrespective of the ongoing criminal process."[149]

- Karthick Theodore v. Madras High Court[150]

The Madras High Court refused to direct to remove the name from the Court orders, the name of the accused who was acquitted from all charges. The Court observed, "This Court honestly feels that our criminal justice system is yet to reach such standards where courts can venture to pass orders for redaction of name of an accused person on certain objective criteria prescribed by rules or regulations. It will be more appropriate to await the enactment of the Data Protection Act and Rules thereunder, which may provide an objective criterion while dealing with the plea of redaction of names of accused persons who are acquitted from criminal proceedings. If such uniform standards are not followed across the country, the constitutional courts will be riding an unruly horse which will prove to be counterproductive to the existing system."[151]

- Jorawer Singh Mundy v. Union of India and Others[152]

A case was once lodged against the petitioner under the Narcotic Drugs and Psychotropic Substances Act, 1985 and he was later acquitted from all charges against him. However, a google search of his name brought judgment of the same and was disadvantageous to his employment expectations. The Delhi High Court directed Indian Kanoon to block the judgment from appearing in search engines till the final hearing.

Regarding the right to be forgotten, the Hon'ble Supreme Court in the Puttaswamy case[153]observed, "The European Union Regulation of 2016 has recognized what has been termed as 'the right to be forgotten'. This does not mean that all aspects of earlier existence are to be obliterated, as some may have a social ramification. If we were to recognize a similar right, it would only mean that an individual who is no longer desirous of his personal data to

[149] Id, Para 16

[150] 2021 SCC Online Mad 2755

[151] Id, Para 37

[152] 2021 SCC Online Del 2306

[153] (2017) 10 SCC 1

be processed or stored, should be able to remove it from the system where the personal data/ information is no longer necessary, relevant, or is incorrect and serves no legitimate interest. Such a right cannot be exercised where the information/ data is necessary, for exercising the right of freedom of expression and information, for compliance with legal obligations, for the performance of a task carried out in public interest, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims. Such justifications would be valid in all cases of breach of privacy, including breaches of data privacy." [154]

3.8. RIGHT TO ERASURE

Right to erasure is used synonymously with right to be forgotten or right to oblivion in most of the legal systems. Article 17 of the GDPR states about Right to Erasure also known as Right to be forgotten. However, under the draft Data Protection Bill, 2019, both right to be forgotten and right to erasure are used in different contexts. Sec 18[155] of the draft Personal Data Protection Bill provides for the 'Right to Correction and Erasure' and Sec 20[156] provides for the 'Right to be Forgotten', which will be discussed in the coming chapters.

3.9. CONCLUSION

The growth of digital age has made us dependant on the internet and the services it offers. In spite of our successful acclimatization with technology in many contexts, it won't be wise if

[154] (2017) 10 SCC 1, Para 636

[155] 18. (*1*) The data principal shall where necessary, having regard to the purposes for which personal data is being processed, subject to such conditions and in such manner as may be specified by regulations, have the right to—
(*a*) the correction of inaccurate or misleading personal data;
(*b*) the completion of incomplete personal data;
(*c*) the updating of personal data that is out-of-date; and
(*d*) the erasure of personal data which is no longer necessary for the purpose for which it was processed.

[156] 20(1) The data principal shall have the right to restrict or prevent the continuing disclosure of his personal data by a data fiduciary where such disclosure—
(*a*) has served the purpose for which it was collected or is no longer necessary for the purpose;
(*b*) was made with the consent of the data principal under section 11 and such consent has since been withdrawn; or
(*c*) was made contrary to the provisions of this Act or any other law for the time being in force.

we fail to recognise the transition to the electronic way of life.[157] Many a time we are unaware of our data being collected. Data privacy is quintessential for human dignity and individual autonomy. We have the right to know how the data collected are being used whether by government or private entities. The eternal storage of data is not acceptable for a society that is evolving. Man is blessed with the virtue of obliteration, to move ahead in life. Quoting Friedrich Nietzsche: "Without forgetting it is quite impossible to live at all." Certain things have to be forgotten, for a better future while certain other matters need to be remembered. This right to some extent prevents data from being transferred into digital eternity. In an era where any update, post or tweet may end up to be part of the eternal internet; the persons who intend to remove those offending data of them shall be given a right to do so, provided law permits it. On the other hand, the information for public good needs to be maintained. Yes, right to privacy has to be protected without estranging societal peace, harmony and security.

[157] ARTHUR R. MILLER, THE ASSAULT ON PRIVACY, 39 (Ann Arbour, Michigan University Press, 1971)

CHAPTER 4

COMPARATIVE ANALYSIS OF DATA PROTECTION LAWS IN VARIOUS JURISDICTIONS

'**Nowadays, digital evolution must no longer be a customer trade-off between privacy and security. Privacy is not a product to sell, it's a valuable asset to protect'**[158].

4.1. INTRODUCTION

With the exponential growth of digitalisation everywhere the need for securing data is high. The focus of governments around the world has changed from cyberspace regulation to citizen rights protection. Though most developing countries, like India, are still in the early stages of drafting legislation, many developed countries, such as the United Kingdom, Australia and the United States, have already set the bar in this area. The US has a sectoral legislation and several federal laws for the protection of privacy, the UK Data Protection Act, 2018 finds its roots in the EU GDPR and Australian data privacy framework is enumerated from the OECD principles.

4.2. DATA PROTECTION IN THE US

The US follows a sectoral approach to data protection legislations. There is no all-encompassing federal law for data protection. The federal law, instead, protects data within sector specific contexts. These statutes apply only to specific sectors like 'healthcare, education, communication, financial services, in case of data collection, to children'.[159]

To put it another way, most privacy laws in the United States restrict data processing based on the context in which data are utilised (e.g., healthcare, banking, education).[160] Essentially, privacy regulation in the United States is highly contextual, sectoral, grounded on common

[158] Stephane Nappo, March 25, 2018, https://www.linkedin.com/pulse/digital-freedom-stops-where-users-begins-st%C3%A9phane-nappo (visited on 20/08/2021)

[159] Terry N, *Existential challenges for health care data protection in the United States*, 3 Ethics Med Public Health 19 (2017)

[160] Schwartz P, Solove D, *Reconciling personal information in the United States and European Union*, 102 Calif L Rev 877–916 (2014)

law, federal and state laws and mostly reliant on private law or explicit agreements later enforced by federal or state legislation. [161] The Federal Trade Commission (FTC) is in charge of federal law enforcement, but state attorneys general are also involved in consumer privacy protection.[162] The Fair Information Practice Principles, that provide a standard set of principles that have formed the foundation for many privacy and data protection laws around the world, including those in the United States, the European Union, and elsewhere, were first laid out in 1973 by an advisory committee of the United States Department of Health, Education, and Welfare[163] and later included in the United States Privacy Act of 1974. [164]

4.2.i. Fourth Amendment

The frontiers of the privacy rights in US are enumerated by the Fourth Amendment to the US Constitution. It protects individuals against 'unreasonable searches and seizures' by the government. In Katz v. United States[165], the Supreme Court ruled that the government's warrantless wiretapping of a person making a phone call from a phone booth went beyond the defendant's subjective expectation of privacy, which might be justified by preventing social norms.[166] A claim for privacy from the Fourth Amendment invokes what is known as the reasonableness standard and the expectation of privacy test. Thus, privacy claims in the US are judged by the standards of an 'objective third party' a person with 'reasonable sensibilities'.

The U.S. Supreme Court has also upheld the privacy rights of individuals around issues such as birth control[167], same-sex relationships[168], and abortion[169], as a *penumbra* of rights derived or implied by the Constitution. These have also been referred to as "unenumerated" rights to privacy.[170]

---

[161] DeVries W, *Protecting privacy in the digital age*, 18 Berkeley Tech LJ 283–311(2003)

[162] ELIF KIESOW CORTEZ, DATA PROTECTION AROUND THE WORLD-PRIVACY LAWS IN ACTION, 232

[163] Sec'y Advisory Comm. On Automated Personal Data Sys., U.S. Dept. of Health, Educ.&Welfare, Records, Computers, and the Rights of Citizens (1973) https://aspe.hhs.gov/report/records-computers-and-rights-citizens. (visited on 21/08/2021)

[164] Privacy Act of 1974, 5 U.S.C. § 552a, as amended.

[165] 389 U.S. 347 (1967)

[166] 389 U.S. 347, 361 (1967)

[167] Griswold v Connecticut, 381 U.S. 479 (1965);

[168] Lawrence v Texas, 539 U.S. 558 (2003);

[169] Roe v Wade, 410 U.S. 113 (1973)

[170] Helscher D, *Griswold v. Connecticut and the unenumerated right of privacy*, 15 N Ill U L Rev 33–61 (1994)

4.2.ii.Privacy torts

Most states have adopted privacy torts, which provide essential privacy rights in the United States, either through common law or legislation, or by interpreting their state constitutions.[171] Privacy torts include intrusion upon seclusion,[172] public disclosure of private facts,[173]appropriation,[174] and false light.[175] These torts safeguard four distinct rights of individuals, all of which revolve around "the right to be left alone," as Samuel Warren and Louis Brandeis famously put it in an 1890 law review article. [176] The reasonableness threshold established in US common law, as well as the First Amendment, have both limited the scope of privacy torts.[177]

4.2.iii. Sectoral laws

The most distinguished character of US privacy and data protection law is the scope or area of regulation. U.S. privacy laws/ regulations are basically of sectoral orientation. For instance, distinct regulations are employed to the data processing undertakings of government agencies and private companies.[178] Further, businesses that are positioned within several sectors of the economy or those process various types of data are governed by different rules.[179] Hence, sectoral laws define the suitable level of protections for discrete/diverse data processing functions, from consumer transactions to law enforcement and maintenance of health records.[180] In a nutshell, sectoral regulations treat threats to privacy and data protection as being specific to certain types of data processing industries or technology.[181]

The various sectoral legislations for data protection are discussed below.

---

[171] Cortez, *supra* note 162 at 235

[172]Restatement (Second) of Torts § 652B (1977).
[173] Restatement (Second) of Torts § 652D (1977).
[174]Restatement (Second) of Torts § 652C (1977).
[175] Restatement (Second) of Torts § 652E (1977).

[176] Brandeis, *supra* note 3

[177] Cortez, *supra* note 162 at 235

[178] Schwartz P, *The EU-US privacy collision: A turn to institutions and procedures*, 126 Harv L Rev 1966–2009(2013)
[179] Id

[180] SWIRE P AND AHMAD K, FOUNDATIONS OF INFORMATION PRIVACY AND DATA PROTECTION: A SURVEY OF GLOBAL CONCEPTS, LAWS AND PRACTICES. (International Association of Privacy Professionals, Portsmouth, 2012)
[181] Reidenberg J, *Resolving conflicting international data privacy rules in cyberspace*, 52 Stan L Rev 1315–1371 (2000)

- **Health Insurance Portability and Accountability Act (HIPAA) [182]**

The HIPAA applies to all Covered entities that collect, maintain, use or disclose personal health information.[183] A Covered Entity is defined as a (1) health plan, (2) health care clearing house or (3) health care provider who transmits any health information in electronic form in connection with a transaction covered by the law.[184] HIPAA requires Covered Entities to follow the Privacy and Security Rules. Under the Privacy Rule, Covered Entities are prohibited from using or disclosing Protected Health Information except in limited circumstances or when the patient or participant has given their consent. By imposing reasonable and suitable administrative, physical, and technical measures, Covered Entities must ensure the confidentiality, integrity, and availability of electronic Protected Health Information that they keep or transfer under the Security Rule.[185]

Under the Act there is protected health information (PHI) and "electronic Protected Health Information"(e-PHI). While HIPPA protects PHI, there are additional requirements that apply to e-PHI.

'Protected health information' means individually identifiable health information:

(1) Except as provided in paragraph

(2) of this definition,[186] that is: (i) Transmitted

by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium[187]

The Security Rule establishes the minimum requirements for all health care entities and contractors which require all data processors to (1) adopt administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of the information; and (2) report security incidents.[188]

---

[182] 42 U.S.C. §1301 et seq.)

[183] Available at: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/privacyrule/prdecember2000all8parts.pdf, accessed on 20/08/2021, 8:28pm, *Id.* at § 160.102.

[184] *Id.* at § 160.104.

[185] *Id.* at §§ 164.302-.318.

[186] "(2) Protected health information excludes individually identifiable health information in: (i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) Records described at 20 U.S.C. 1232g (a)(4)(B)(iv); and (iii) Employment records held by a covered entity in its role as employer." See §160.103.

[187] Individually identifiable health information includes demographic data, that relates to: the individual's past, present or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. See 45 CFR 160.103.

[188] Eisenhauer MP (2007) Managing your data processors: legal requirements and practical solutions. BNAI's World Data Protection Report.

- **Controlling the Assault of Non-Solicited Pornography and Marketing Act, 2003** (CAN-SPAM Act)

The collecting and use of e-mail addresses is governed by this Act. Covers all commercial messages, which are defined by the legislation as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service" including email that promotes material on commercial websites.[189] Commercial email must include non-deceptive sender and subject information; opt-out provisions; sender's address; and clear and conspicuous identification that the e-mail is an advertisement or solicitation.[190] The Act imposes criminal penalties on individuals who harvest email addresses or generate them through a dictionary attack.[191]

All organisations, including 501(c)(3) organisations, are required by the CAN-SPAM Act to not send emails with materially false, misleading, or deceptive information in the header or subject line.[192]Thus, if an email is an advertisement or solicitation, it must clearly identify itself as such. The email must contain 'clear and conspicuous' notice of the opportunity to opt-out of receiving future emails from the sender, and must include some type of return email address or other mechanism whereby the recipient is in fact able to opt-out.[193] The sender's physical postal address must be included in the email. Finally, senders must honour recipients' decisions to opt out of receiving further emails from the sender.[194]

- **The Fair Credit Reporting Act[195] (and the Fair and Accurate Credit Transactions Act (Pub. L. No. 108–159) which amended the Fair Credit Reporting Act)**

---

http://www.privacystudio.com/Links%20posted%20to%20web/BNAI%20%20Managing%20Data%20Processors%20Aug%2007.pdf

[189] 15 USC §7702, http://uscode.house.gov/view.xhtml?hl=false&edition=prelim&req=granuleid%3AUSC-prelimtitle15section7702&f=treesort&fq=true&num=0&saved=%7CY2FuIHNwYW0gYWN0%7CdHJlZXNvcnQ%3D%7CdHJ1ZQ%3D%3D%7C0%7Ctrue%7Cprelim

[190] 15 U.S.C. §§7701–7713.

[191] "CAN-SPAM Act: A Compliance Guide for Business", Federal Trade Commission. Available at: https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guidebusiness. (last visited on 25/08/2021, 10:00 am)

[192] *Id*. at §§ 7704(a)(1)-(2).

[193] *Id*. at § 7704(a)(3).

[194] *Id*. at § 7704(a)(4).

[195] 15 U.S.C. §1681

Consumer reporting agencies, people who use consumer reports (such as lenders), and those who offer consumer reporting information are all included (such as a credit card company). "Consumer reports" are any communication issued by a consumer reporting agency (CRA) regarding a consumer's creditworthiness, credit history, credit capacity, character, and general reputation that is used to evaluate a consumer's eligibility for credit or insurance[196]. A CRA must, "follow reasonable procedures to assure accuracy of the information."[197] Where data are "inaccurate or incomplete or cannot be verified", a CRA must immediately correct the data[198]

- **Electronic Communications Privacy Act, 1986[199]**

Prohibits wiretaps of communications of others without court approval without a party's prior consent. Prohibits the use or disclose any information acquired by illegal wiretapping or electronic eavesdropping[200].

- **Computer Fraud and Abuse Act, 1986[201]**

Seeks to prevent and punish hacking related activities which the Act defines as "unauthorized access" to protected computers.[202] In addition, the Act bars individuals or entities from exceeding the scope of their "authorized access"[203]. "Protected computers" includes: those used by financial institutions, the U.S. government, and computers used in or affecting interstate or foreign commerce or communication[204]. The Act defines "damage" as any impairment to the integrity or availability of data, a program, a system, or information[205].

- **Family Education Rights and Privacy Act, 1974**

[196] 15 U.S.C. § 1681(d)(1).

[197] 15 U.S.C. § 1681e (2013).

[198] 15 U.S.C. § 1681i (a)(5)(A) (2013).

[199] 18 U.S.C. §2510

[200] Doyle C (2012) Privacy: an overview of the Electronic Communications Privacy Act. Congressional Research Service, p i. https://www.hsdl.org/?view&did¼725508

[201] 18 U.S.C. §1030

[202]18 U.S.C. § 1030.
[203]18 U.S.C. § 1030(e)(6).
[204]18 U.S.C. § 1030(e)(2).
[205] 18 U.S.C. §1030(a)(5).

The Family Educational Rights and Privacy Act[206] (FERPA) protects the data included in students educational records and applies to all educational agencies and institutions that receive applicable funding from the U.S. Department of Education, including non-profits.[207] Under this law "educational records" are defined as records, files, documents and other materials that contain information directly related to a student that are maintained by an educational agency or institution or by a person acting for such agency or institution.[208]An educational agency or institution is defined as any public or private agency or institution which is the recipient of funds under any applicable government program.[209]

Under FERPA, any school which receives educational funds from the government must grant the parents of students, or the students themselves if they are over the age of eighteen, the right to review and inspect student's educational records. Each educational agency or institution is directed to establish necessary procedures for granting such requests within a reasonable time, but in no case more than forty-five days after the request is made.[210] In addition, FERPA mandates that the educational agency or institution must obtain written consent from a parent, guardian or eligible student before releasing education records or personally identifiable information contained therein to any individual, agency or organization, other than to a list of specifically excluded individuals and related state agencies or officials.[211]

- **Children's Online Privacy Protection Act, 1998[212] (COPPA)**

The COPAA was designed to safeguard children under the age of thirteen when they use the Internet by governing how websites acquire, use, and disclose personal information about them.[213] Under COPPA, a website's "operator"[214] must inform the child's parent of its data

[206] 20 USC § 1232g

[207] *Id.* at § 1232g(a)(3).

[208] *Id.* at § 1232g(a)(1)(D)(3).

[209] *Id.*

[210] *Id.* at § 1232g(a)(1)(A).

[211] *Id.* at § 1232g(b).

[212] 15 U.S.C. §§ 6501, *et seq*,

[213] Robert Hasty Et.al, *Data Protection Law In USA*, Advocates for International Development, https://www.neighborhoodindicators.org/sites/default/files/course-materials/A4ID_DataProtectionLaw%20.pdf (visited on 22/08/2021)

[214] 16 C.F.R. pt 312.2.

collection policies and seek parental consent before collecting the information. [215] If the operator has real knowledge that the website is collecting children's personal information, COPPA applies to both children's websites and "general audience" websites. [216]

- **Gramm-Leach- Bliley Act, 1999 [217] (GLBA)**

The GLBA requires that financial institutions 'respect the privacy of its customers and protect the security and confidentiality of those customers' non-public personal information.[218] Financial institutions may transfer personal information to other companies if it is necessary to the performed financial services. Information may be shared with credit reporting agencies or financial regulatory agencies.[219]

4.2.iv. The Federal Trade Commission

The Federal Trade Commission (FTC) regulates the processing of personal information in the United States, and it plays an important role in preserving the privacy of American customers.[220] It does so primarily through Section 5 of the Federal Trade Commission Act, which gives it the authority to maintain independent oversight of and take enforcement action against unfair and deceptive commercial practises. [221] The FTC has the power to issue injunctions and civil penalties against businesses that breach customers' privacy rights, and it now "dominate[s] the enforcement of privacy rules." [222] While the FTC has been credited for influencing big corporations' behaviour, it has also been chastised for failing to act on highly criticised actions that have created privacy issues, such as Facebook's online monitoring methods. [223] The FTC is the primary enforcement authority for federal privacy laws such

[215] *Id.* at pts. 312.4(c), 312.5.

[216] *Id.* at pt. 312.3.

[217] *Id.* at § 6801, *et seq.*

[218] *Id*. at § 6801(a).

[219] DARIO MAURA VINCETE & SOFIA DE VASCONSELS, DATA PROTECTION IN THE INTERNET, 412 (Springer 2020)

[220] HOOFNAGLE C, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY, (Cambridge University Press, New York , 2016)

[221] 15 U.S.C § 45.

[222] Solove D, HartzogW, *The FTC and the new common law of privacy*, 114 Colum L Rev 583–676 (2014)

[223] Cortez, *supra* note 162 at 235

GLBA,[224] FCRA,[225]and COPPA[226]. In recent years, it has taken a more active role in protecting consumer privacy by issuing consent decrees in settlements with firms accused of violating privacy laws.[227]

Apart from these federal laws various state laws are also there. The most relevant among them is the California Consumer Privacy Act (CCPA).

California Consumer Privacy Act (CCPA)[228]

California's implementation of the CCPA, a comprehensive privacy statute that critics have dubbed "California's GDPR," is by far the most significant recent privacy development in the United States. The CCPA is having a wide influence due to California's size and the fact that it is home to Silicon Valley, and businesses across the United States and around the world are assessing what it means for them.[229]

The CCPA came into effect on 1 January 2020, and immediately became the most far- reaching privacy or data protection law in the Country. The CCPA applies to for-profit entities that do business in California, which collect or determine how personal information is processed, and fall within one of three size categories. It imposes stringent privacy policy disclosure obligations on businesses that gather personal data from California residents. It requires businesses to give California residents with the ability to access and delete their personal information, as well as the ability to prevent their information from being sold to third parties. It bans firms from selling personal information about children under the age of 16 without their express consent. The CCPA creates a private right of action for certain data breaches caused by a company's failure to follow and maintain acceptable security rules and practises. The California Attorney General is authorised to enforce the CCPA's requirements with statutory fines of up to $7,500 per infringement.

[224] 15 U.S.C. §§ 6801-6809 (2012).
[225] 15 U.S.C. § 1681 (2012).
[226] 15 U.S.C. §§ 6501-6506 (2012).

[227] Robert Hasty Et.al, supra note 210

[228] The California Consumer Privacy Act (CCPA), A.B. 375, 2017 General Assembly, Reg., Session, (Cal.2018)
[229]ALEN CHARLES RAUL, THE PRIVACY, DATA PROTECTION AND CYBER SECURITY LAW REVIEW, 416 (The Law Reviews, 2019)

4.3. DATA PROTECTION IN UK

The primary data protection legislation in the UK was the Data Protection Act 1998[230] (DPA 1998), prior to 2016. The DPA 1998 was enacted in order to implement the 1995 EU Data Protection Directive (DPD) in UK domestic law.[231] In 2016, the EU General Data Protection Regulation (GDPR) was enacted, repealing the DPD.[232] The UK Government has transferred the General Data Protection Regulation (Regulation (EU) 2016/679) into UK national law (forming the "UK GDPR") following the UK's exit from the European Union. In order to account for its status as a national law of the United Kingdom, the UK has made a number of technical adjustments to the GDPR (for example, changing references to "Member State" to "the United Kingdom"). The Data Protection, Privacy, and Electronic Communications (Amendments and Other Provisions) (EU Exit) Regulations 2019 were used to make these modifications. At this point, all material duties on controllers and processors under the UK GDPR and the EU GDPR are fundamentally the same.[233]

The Data Protection Act of 2018 ("DPA") remains in effect as a national data protection law that supplements the GDPR regime in the United Kingdom. It addresses issues that were previously allowed derogations and exclusions from the EU GDPR (for example, strong public interest justifications for processing special category data and context-specific exemptions from elements of the GDPR such data subject rights).[234] This new data protection regime under the GDPR and DPA 2018 is largely similar to the one it replaced, although some changes have been introduced.[235] The DPA 2018 is divided into six main parts: general processing, law enforcement processing, intelligence service processing, the UK data supervisory authority, the

[230] Data Protection Act, 1998

[231]Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31.

[232]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L 119/1. After the transition period of the UK's withdrawal from the EU, the 'UK GDPR' will replace the GDPR in the UK – the UK GDPR is essentially the GDPR converted into domestic legislation: see The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019, sch 1.

[233] Data Protection Laws of the World, DLA Piper, 883

[234] Id

235 Benjamin Wong, The journalism exception in UK data protection law, 12:2, Journal of Media Law, 216-236, (2020)

Information Commissioner's Office (ICO), enforcement and supplementary and final provisions. [236]

The Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended by the Privacy and Electronic Communications (EC Directive) (Amendments) (Regulations 2011) (PECR) regulate direct marketing, but also the processing of location and traffic data and the use of cookies and similar technologies. The European Commission issued a draft of the proposed Regulation on Privacy and Electronic Communications (ePrivacy Regulation) to replace the existing ePrivacy Directive. [237] Since the eRegulation has not yet been force, it is a question whether the UK will comply to it in the Post-Brexit scenario.

The key changes in the proposed ePrivacy Regulation will:

a) Make consent for cookies more difficult to obtain.
b) Attempt to shift the burden of obtaining consent for the use of cookies to website browsers.
c) Make consent for direct marketing more difficult to obtain and require it to meet the GDPR standard; however, existing exceptions are likely to be retained.[238]

The Data Protection Act 2018 regulates the use of personal information by organisations, businesses or government. The **Data Protection Act 2018** contains four parts that create four different "data protection regimes" within the UK:

1. Part one is structured around the European GDPR, supplementing and tailoring it into domestic UK law.
2. Part two extends beyond the EU GDPR and modifies it in certain cases to apply differently to UK law.
3. Part three creates a new and separate regime for law enforcement authorities.
4. Part four creates a new and separate regime for the UK's intelligence services.

The **Data Protection Act 2018** also adopts the central definitions of the EU GDPR[239], such as:

[236] Alen Charles, supra note 226 at 374

[237] Id

[238] Id

[239] Sec 5 of the DPA, 2018

- Personal data[240] meaning "any information relating to an identified or identifiable living individual."
- Processing[241] meaning *"an operation or set of operations which is performed on information,"* such as collection, recording, storage, disclosure, combination etc.
- Data subject meaning[242] *"living individual to whom personal data relates."*
- Controller and processor[243] meaning the *"natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data."*

4.3.i. Data Protection Principles

The DPA has laid down certain principles known as the 'Data Protection Principles'. They are

1. The first data protection principle is that the processing of personal data for any of the law enforcement purposes must be lawful and fair.[244]

2. The second principle states that the purpose for which data is collected must be specific, legitimate and explicit.[245]

[240] Sec 3 (2) "Personal data" means any information relating to an identified or identifiable living individual (subject to subsection (14)(c)) and Sec 3(3) "Identifiable living individual" means a living individual who can be identified, directly or indirectly, in particular by reference to—

(a)an identifier such as a name, an identification number, location data or an online identifier, or

(b)one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

[241] Sec 3(4)

[242] Sec 3(5)

[243] Sec 3(6)

[244] S. 35

[245] S. 36-The second data protection principle

(1)The second data protection principle is that—

(a)the law enforcement purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and

(b)personal data so collected must not be processed in a manner that is incompatible with the purpose for which it was collected.

3. The third data protection principle is that personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed.[246]
4. The fourth principle provides for erasure or rectification of inaccurate personal data.[247]
5. The fifth data protection principle is that personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed.[248]
6. The sixth data protection principle is that personal data processed for any of the law enforcement purposes must be so processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures.[249]

4.3.ii. Information Commissioner's Office

The DPA stipulates the Information Commissioner's Office (ICO)[250]as the main data protection authority in UK. The Act frames the role, jurisdiction, function and powers of the ICO.[251] The DPA 2018 is enforced by the ICO and, the ICO has powers of enforcement in relation to organisations complying with the data protection requirements in the GDPR.

The ICO has independent status and is responsible for

a) maintaining the public register of controllers

[246] S. 37

[247] S. 38- The fourth data protection principle

(1)The fourth data protection principle is that—

(a)personal data processed for any of the law enforcement purposes must be accurate and, where necessary, kept up to date, and

(b)every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay.

[248] S. 39

[249] S. 40

[250] S. 114 of the DPA, 2018

[251] S.115 and 116 of the DPA, 2018

b) supporting good practise by providing data protection advice and guidance and working with organisations to enhance their data processing practises through audits, advisory visits, and data protection workshops

c) ruling on complaints

d) taking regulatory actions.

4.3.iii.Rights of the Data Subject

Data subjects have a set of rights to govern how their personal data is processed that are similar to those in the EU GDPR. Controllers are required to disclose information on actions done in response to requests within one calendar month by default, with the controller having a limited ability to extend this period by two months if the request is onerous**.**

- Right of access[252]

A data subject has the right to seek access to and a copy of his or her personal data, along with the prescribed information about how the controller has used the data.

- Right to rectify[253]

Data subjects have the right to have erroneous or incomplete personal data rectified or updated as soon as possible.

- Right to erasure[254] ('right to be forgotten')

Data subjects have the right to have their personal data erased. The right is not absolute; it only applies in a limited set of circumstances, such as when the controller no longer requires the data for the purposes for which they were collected or otherwise lawfully processed, or as a result of the controller's successful exercise of the right to object or withdrawal of consent.

- Right to restriction of processing[255]

In certain cases, data subjects have the right to restrict the processing of their personal data. These include situations where the data's accuracy is questioned, the processing is illegal, the data are no longer needed except for the data subject's legal claims, or the controller's legitimate grounds for processing are questioned.

[252] Article 15 of EU GDPR and Art 45 of DPA, 2018

[253] Article 16 of EU GDPR and Art 46 of DPA, 2018

[254] Article 17 of EU GDPR and Art 47 of DPA, 2018

[255] Article 18 of EU GDPR and Art 47 of DPA, 2018

- Right to data portability[256]

The data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used, and machine-readable format where the processing of personal data is legitimised either on the basis of the data subject's assent to processing or where processing is essential for the performance of a contract.

- Right to object[257]

When processing is done on the legal basis of the data controller's legitimate interests or in the public interest, data subjects have the right to object to processing. Controllers will be required to halt data processing until they can demonstrate "compelling legitimate reasons" for processing that outweigh the data subject's rights. Furthermore, data subjects have an unrestricted right to object at any time to the processing of their personal data for direct marketing purposes.

- The right not to be subject to automated decision making, including profiling [258]

  Automated decision-making (including profiling), that significantly affect the data subject is only permitted when it is "required for entering into or completing a contract, permissible by UK law, or the data subject has given explicit (i.e. opt-in) consent."

4.3.iv. Enforcement Agencies

The ICO has a range of enforcement powers under the DPA 2018, including monitoring and enforcement of the GDPR and the DPA 2018 in the UK. Such monitoring and enforcement powers include the power to issue:

a) information notices[259] - requiring controllers and processors to provide the ICO with information that the Commissioner reasonably requires in order to assess compliance with the GDPR or DPA 2018.

[256] Article 20

[257] Article 21

[258] Article 22 of EU GDPR and Art 49 of DPA, 2018

[259] Sec 142-145 of DPA, 2018

b) assessment notice[260]: requiring the controller or processor to permit the ICO to carry out an assessment of whether the controller or processor is in compliance with the GDPR or DPA 2018

c) notice of intent[261]: where, after conducting its investigation, the ICO issues a notice of intent to fine the controller or processor in relation to a breach of the GDPR or the DPA 2018. Such a notice sets out the ICOs areas of concern with respect to potential noncompliance of the GDPR or the DPA 2018 and grants the controller or processor the right to make representations. After such representations have been carefully considered, the ICO reaches its final decision on any enforcement action in the form of an enforcement notice.

d) enforcement notices[262]: such notices are issued where the ICO has concluded the controller or processor has failed to comply with the GDPR or the DPA 2018, setting out the consequences of non-compliance, which could include a potential ban on processing all or certain categories of personal data; and

e) penalty notices[263]: if the ICO is satisfied that the controller or processor has failed to comply with the GDPR or the DPA 2018, or has failed to comply with an information notice, an assessment notice or an enforcement notice, the ICO may, by written notice, require a monetary penalty to be paid for failing to comply with the GDPR or the DPA, 2018. Under the GDPR, such monetary penalties can amount to €20 million or 4 percent of annual worldwide turnover.

Though the status of data protection laws in UK post-Brexit is still uncertain, its expected that EU GDPR would have legal effects in UK until the UK government introduce legislation repealing the provisions and legal effect of the GDPR in UK law and amend the provisions of the DPA 2018, as the GDPR came into force before UK's scheduled departure from EU.[264]

[260] Sec 146 and 147 of DPA, 2018

[261] Schedule 16 of DPA, 2018

[262] Sec 149-153 of DPA, 2018

[263] Sec 155-157 of DPA, 2018

[264] Alen Charles, supra note 226 at 398

4.4. DATA PROTECTION LAWS IN AUSTRALIA

In Australia, information privacy is secured by a combination of Commonwealth, State, and Territory legislation, each of which provides a set of privacy standards based on the Organisation for Economic Co-operation and Development (OECD) Guidelines[265] on the Protection of Privacy and Transborder Flows of Personal Information (OECD Principles).[266] Information privacy protection in Australia has been described as a "patchwork." Although all pertinent laws are based on the OECD Principles, there still are substantial variances in how they are applied from jurisdiction to jurisdiction, and there are certain overlaps between Commonwealth and State legislation (especially in the area of health privacy). [267]A Commissioner oversees each of Australia's information privacy regimes. In general terms, Privacy Commissioners are charged with addressing privacy issues - usually through a conciliation procedure. The Information Commissioner has a responsibility at the

[265] Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 13-16 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD, 2001).
1. Collection limitation principle: There should be limits to the collection of personal data. Any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2. Data quality principle: Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
3. Purpose specification principle: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4. Use limitation principle: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with purpose specification principle except: a) with the consent of the data subject; or b) by the authority of law.
5. Security safeguards principle: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.
6. Openness principle: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
7. Individual participation principle: An individual should have the right:
a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
b) to have communicated to him, data relating to him:
i) within a reasonable time;
ii) at a charge, if any, that is not excessive;
iii) in a reasonable manner; and
iv) in a form that is readily intelligible to him;
c) to be given reasons if such a request is denied, and to be able to challenge such denial; and
d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
8. Accountability principle: A data controller should be accountable for complying with measures which give effect to the principles stated above.

[266] Paterson & McDonagh, *supra* note 110

[267] David Watts and Pompeu Casanovas, *Privacy and Data Protection in Australia: a Critical overview (extended abstract), (*visited on 25/08/2021) https://www.w3.org/2018/vocabws/papers/watts-casanovas.pdf

Commonwealth level in commencing enforcement procedures that can result in fines of up to $A2,100,000.00.[268]

The Privacy Act 1988 (Privacy Act) is the principal piece of Australian legislation protecting the handling of personal information about individuals. This includes the collection, use, storage and disclosure of personal information in the federal public sector and in the private sector.[269] Privacy Act protects the personal information i.e., information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not.[270] It gives sensitive information[271] a heightened level of protection.

The Privacy Act is intended to regulate the handling of personal information through a set of information privacy principles that govern various aspects of information handling, such as principles that limit the collection, use, and disclosure of personal information, principles that make information controlling more transparent, and principles that necessitates organizations to maintain personal information secure. In the context of those categories of personal information that also qualify as "sensitive information," the restrictions on collection, use, and disclosure are more stringent.

---

[268] Id

[269] Australian Government- Federal Register of Legislation, https://www.legislation.gov.au/Details/C2021C00242, (last visited on 22/08/2021 10:30 am)

[270] Sec 6 the Data Privacy Act, 1988

[271] Sec 6 of the Data Privacy Act, 1988, *sensitive information* means:

(a) information or an opinion about an individual's:
  (i) racial or ethnic origin; or
  (ii) political opinions; or
  (iii) membership of a political association; or
  (iv) religious beliefs or affiliations; or
  (v) philosophical beliefs; or
  (vi) membership of a professional or trade association; or
  (vii) membership of a trade union; or
  (viii) sexual orientation or practices; or
  (ix) criminal record;
  that is also personal information; or
(b) health information about an individual; or
(c) genetic information about an individual that is not otherwise health information; or
(d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
(e) biometric templates.

The Privacy Act applies to Australian Privacy Principles (APP) entities and extends to all of Australia's external Territories.[272] An APP entity means an agency or organisation. The Privacy Act also applies to an act done, or practice engaged in, or outside Australia (and Australia's external Territories) by an organisation, or small business operator, that has an Australian link (in other words is considered an APP entity).[273]

The Privacy Act provides 13 Australian Privacy Principles which mandates on government and private organisations collecting, handling, storing, using and disclosing personal information to follow certain guidelines and guarantees certain rights to the individuals to access and correct personal information. The Australian Privacy Principles[274] are:

- **Australian Privacy Principle 1—open and transparent management of personal information**- Organisations must take reasonable steps to implement practices, procedures and systems that ensure compliance with APPS and must manage personal information in an open and transparent way.[275]

- **Australian Privacy Principle 2—anonymity and pseudonymity**.

Individuals must have the option of not identifying themselves unless this is impracticable.[276]

- **Australian Privacy Principle 3—collection of solicited personal information**

information may be collected only if it is reasonably essential for the organisation's functions or operations and must be collected only by lawful and fair means.[277]

- **Australian Privacy Principle 4—dealing with unsolicited personal information**

[272] Sec 5 A, Privacy Act, 1988

[273] One Trust Data Guidance, Comparing Privacy Laws: GDPR v. Australian Privacy Act, https://www.dataguidance.com/sites/default/files/gdpr_v_australia.pdf (last visited on 22/08/2021 11:00 am)

[274] Schedule 1, Privacy Act 1988, https://www.legislation.gov.au/Details/C2014C00076 (last visited on 22/08/2021 10:00 am)

[275] APP 1.1

[276] APP 2.1

[277] APP 3.1 and 3.2

When an organisation receives unsolicited personal information, it must consider whether it could have gathered the information itself under the APPs within a reasonable time.[278] If not, the organisation must destroy or 'de-identify' that information.[279]

- **Australian Privacy Principle 5—notification of the collection of personal information**

An organisation collecting personal information must take reasonable steps (if any) to make the individual aware of a number of mandated issues at or before the time of collection (or as soon as practical thereafter);[280] for example: the organization's identity; the purpose of the collection; the types of organisations to whom the personal information may be disclosed; whether the organisation is likely to disclose the information to overseas recipients (and, if so, to which countries); and that the organization's privacy policy contains certain information (e.g., how to make a complaint).[281] When personal information is gathered indirectly rather than directly from an individual, an organisation must take reasonable steps to ensure that the individual is aware of the same issues.

- **Australian Privacy Principle 6—use or disclosure of personal information**

Personal data shall be used or disclosed solely for the reason for which it was obtained (the primary purpose).[282] Personal data may be used or disclosed for a secondary purpose in the following circumstances:

a) the secondary purpose is related to the primary purpose, and the individual would reasonably expect it to be disclosed or used in this manner;
b) the individual has given agreement to that disclosure or use;
c) or another exception applies (e.g., that the use or disclosure is required by Australian law).[283]

[278] APP 4.1

[279] APP 4.3

[280] APP 5.1

[281] APP 5.2

[282] APP 6.1

[283] APP 6.2

- **Australian Privacy Principle 7—direct marketing**

If an organisation has personal information about an individual, it must not use or disclose that information for direct marketing purposes.[284] An organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing in the circumstances given in APP 7.2.

- **Australian Privacy Principle 8—cross-border disclosure of personal information**

The sharing of information to a person who is located outside of Australia is governed by APP 8. In some instances, an organisation may be held accountable under Section 16C of the Privacy Act for a breach of the APPs by an overseas recipient of personal information supplied by that organisation.

- **Australian Privacy Principle 9—adoption, use or disclosure of government related identifiers**

Unless an exception applies, (e.g., the adoption, disclosure or use is required or authorised by an Australian law) an organisation may not use or disclose an identification assigned to an individual by a government agency as its own identifier of the individual; or reveal or use an identifier assigned to an individual by a government agency as its own identifier of the individual.[285]

- **Australian Privacy Principle 10—quality of personal information**

An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity collects is accurate, up-to-date and complete.[286]

- **Australian Privacy Principle 11—security of personal information**

If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:

[284] APP 7.1

[285] Allens, *In a nutshell: data protection, privacy and cybersecurity in Australia*, Lexology, (October 2020) https://www.lexology.com/library/detail.aspx?g=2027ba56-6178-4e7f-9273-9aa9bb2f5066

[286] APP 10.1

(a) from misuse, interference and loss; and

(b) from unauthorised access, modification or disclosure.[287]

- **Australian Privacy Principle 12—access to personal information**

In general, an organisation must provide an individual with access to any personal information maintained about him or her upon request. There are several exceptions to this general rule, such as where providing access to personal information would have an unreasonable impact on other people's privacy, or when limiting access is mandated or authorised by Australian law.

- **Australian Privacy Principle 13—correction of personal information**

If the entity is satisfied that the information is erroneous, or if the individual requests it, the entity shall take reasonable steps to correct the information. According to the Guidelines, "appropriate... deletions" may be among the reasonable procedures to be done. Individuals, on the other hand, do not have an express legal right to have erroneous data removed. In fact, under Australian law, there is currently no right to have data removed.

If an organisation refuses to rectify personal information, it must explain why and inform the individual who sought the correction of the methods available to file a complaint.

The Office of the Australian Information Commissioner is the authority under the Privacy Act to regulate data protection in Australia.[288] It is the authority responsible for enforcing the Privacy Act.

On March 12, 2014, significant changes to the Privacy Act took effect in a variety of areas, including direct marketing, privacy collection statements and privacy policies, the collecting of unsolicited personal data, the dissemination of personal data beyond Australia, and credit reporting. Significant penalties can now be applied for "severe" or "repeated" breaches of data subjects' privacy..[289]

Certain organisations are excluded from the duty to comply with the APPs under the Privacy Act. Small business owners (those with an annual turnover of less than A$3 million in the

[287] APP 11.1

[288] Part IV, Privacy Act 1988

[289] *supra* note 274

previous financial year) are normally exempt from the Privacy Act.[290] There are also exemptions for domestic use[291], media organisations[292] and political representatives[293]. There is no general exemption for not-for-profit organisations.

Acts or practises that are directly related to a current or prior job relationship and involve an employee record held by the employer are exempt from the applicability of the Privacy Act.[294] In effect, this implies that the Privacy Act does not apply to many of an organization's operations involving its own personnel.[295] The sharing of personal information (other than sensitive information) between companies in the same corporate group is exempt from the application of the Privacy Act.[296] However, even when information is transferred within group companies, the restrictions regarding the disclosure of personal information outside of Australia continue to apply.

As part of its response to the Australian Competition and Consumer Commission's (ACCC) Digital Platforms Inquiry final report (DPI Report)[297], the Treasury announced commitments to improve consumer protection and rights under privacy laws, as well as increasing penalties for violations.[298] The ACCC published the DPI Report on July 26, 2019, which included 23 recommendations aimed at addressing the influence of digital platforms on consumer rights and competition in the media and advertising industries.[299] The recommendations included increasing penalties, regulating social media privacy, right to erasure, consumer data protection etc. The report also suggested the widening the definition of 'personal information',

[290] Section 6 D

[291] Section 16 of the Privacy Act.

[292] Section 7B(4) of the Privacy Act.

[293] Section 7C(1) of the Privacy Act.

[294] Section 7B(3) of the Privacy Act.

[295] Micheal Morris and Emily Cravigan, *The Privacy, Data Protection and Cyber Security Law Review- Australia,* (last visited on 23/08/2021) https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/australia

[296] Section 13B of the Privacy Act.

[297] https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf

[298] Nitesh Patel and Aayush Jain, *Government to Enhance Data Privacy and to 'Regulate the Digital Age'*, ((last visited on 23/08/2021) https://www.gclegal.com.au/limelight-newsletters/government-to-enhance-data-privacy-and-protection-to-regulate-the-digital-age/?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration

[299] Id

"Clarifying the definition of 'personal information will update the Privacy Act in line with current and future technological developments relating to the scope of technical information collected, used and shared about individuals in the digital economy and is particularly important in light of the large and increasing volume of technical information collected from individuals in Australia".[300] Furthermore, the proposed reforms would allow Australians to request that online platforms stop using or disclosing their personal information, with greater protections if the person is a minor or deemed vulnerable.[301]

4.5. CONCLUSION

Although, in a preliminary examination, the scholars might consider America's privacy protection framework weak than the European approach, however, in some aspects, the American framework offers more protection than the European counterpart.[302] Swire and Kennedy-Mayo[303] argue that

"U.S. protections are stricter in seven ways:

1) oversight of searches by independent judicial officers;

(2) probable cause of a crime as a

relatively strict requirement for both physical and digital searches;

(3) even stricter requirements for government use of telephone wiretaps and other real-time interception;

(4) the exclusionary rule, preventing prosecutors' use of evidence that was illegally obtained, is supplemented by civil suits;

(5) other legal standards that are relatively strict for government

access in many non-search situations, such as the judge-supervised "reasonable and articulable suspicion" standard under ECPA;

(6) transparency requirements, such as notice to the service provider of the legal basis for a request;

---

[300] ACCC, Digital Platforms Inquiry, Final Report, June 2019, Page 462, https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf

[301] Asha Barbaschow, *Australian privacy law amendments to cover data collection and use by digital platforms*, (last visited on 24/08/2021, 11:30 am) https://www.zdnet.com/article/australian-privacy-law-amendment-to-cover-data-collection-and-use-by-digital-platforms/

[302] DARIO MAURA VINCETE & SOFIA DE VASCONSELS, DATA PROTECTION IN THE INTERNET, (Global Studies in Comparative Law, Springer 2020)

[303] Swire P, Kennedy-Mayo D*, How both the EU and the U.S. are "Stricter than Each Other for the Privacy of Government Requests for Information"*, 55 Emory Law J 617 (2017)

(7) lack of data retention requirements for internet communications; and

(8) lack of limits on use of strong encryption."[304]

"In contrast to the European Union's data protection approach, which in many ways represents the gold standard of privacy protections, the dominant approach in the U.S. is grounded in consumer protection regulations."[305]The Privacy Principles under the Australian law and Data Protection Principles under the UK legislation can be considered as a powerful means of protection of data privacy. However, the sectoral legislation in US has an advantage as almost everything is covered in a more efficient manner, though it is complex and costly.

.

[304] Id

[305] McGeveran W, *Friending the privacy regulators*. 58 Arizona Law Review. 959-961, (2016)

CHAPTER 5

CRITICAL ANALYSIS OF DATA PROTECTION BILL, 2019

"Our own information is being weaponised against us with military efficiency. Every day, billions of dollars change hands and countless decisions are made on the basis of our likes and dislikes, our friends and families, our relationships and conversations, our wishes and fears, our hopes and dreams. These scraps of data, each one harmless enough on its own, are carefully assembled, synthesized, traded and sold."[306]

5.1. INTRODUCTION

In 2017, work on the most recent version of the Indian data protection law began. Despite repeated claims that India would have this law in place soon, there has been no progress. The Government of India announced the formation of an expert committee to frame India's data protection law during the Supreme Court hearings in K S Puttaswamy and Anr v Union of India and Ors [307] to clear the judicial uncertainty surrounding the existence of the right to privacy. A 10-member committee led by retired Supreme Court judge B N Srikrishna was created by the Ministry of Electronics and Information Technology (MeitY). This was not the first attempt at drafting a data protection law in India. In reality, there have been numerous similar campaigns and bills throughout the last decade. Justice A P Shah chaired a new group of experts in 2012, which made specific proposals for the creation of a data protection regulation[308].

5.2. DATA PROTECTION BILL, 2019

The committee headed by Justice B.N Srikrishna submitted the Report 'A free and fair digital economy, protecting privacy, empowering Indians' and proposed a draft legislation for Data

[306] Sara Salinas and Sam Meredith, Tim Cook: Personal data collection is being 'weaponized against us with military efficiency'https://www.cnbc.com/2018/10/24/apples-tim-cook-warns-silicon-valley-it-would-be-destructive-to-block-strong-privacy-laws.html, (last visited on 25/08/2021, 09:30 am)

[307] (2017) 10 SCC 1

[308] Report of the Group of Experts on Privacy Constituted by Planning Commission of India under the Chairmanship of Justice A.P Shah, Former Chief Justice, Delhi High Court, https://cis-india.org/internet-governance/blog/report-of-group-of-experts-on-privacy.pdf, (last visited on 25/08/2021, 10:30 am)

Protection, 2018. The Bill though acknowledged was criticised for its data localisation principles. The Data Protection Bill 2019 was the result of such a reinvention making huge changes in various provisions and widening the powers of the Central Government. The Data Protection Bill 2019 establishes a legal framework for the collection and use of personal information. The Bill also proposes the creation of data protection authority for making regulations and enforcing the legal framework.

The preamble to the Bill is as follows, "to provide for protection of the privacy of individuals relating to their personal data, specify the flow and usage of personal data, create a relationship of trust between persons and entities processing the personal data, protect the rights of individuals whose personal data are processed, to create a framework for organisational and technical measures in processing of data, laying down norms for social media intermediary, cross-border transfer, accountability of entities processing personal data, remedies for unauthorised and harmful processing, and to establish a Data Protection Authority of India for the said purposes and for matters connected therewith or incidental thereto."[309]

Personal Data is defined in the Bill as "personal data" means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling;"[310] and "processing" in relation to personal data, means "an operation or set of operations performed on personal data, and may include operations such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction;"[311]

The salient features of the Personal Data Protection Bill 2019 are :

5.2.i. Applicability

The Act applies[312] to the processing of personal data

[309] Preamble, Personal Data Protection Bill 2019

[310] Sec 3 (28) of the Personal Data Protection Bill

[311] Sec 3 (31)

[312] Sec 2

i) where it is collected, disclosed, shared within the territory of India.[313]

ii) by State/Indian Company/citizen of India or any body incorporated under Indian Law.[314]

iii) By data fiduciaries or data processors not present within the territory, if the processing is in connection with any business carried on in India, or any systematic activity of offering goods or services to data principals within the territory of India;[315]

The Act shall not apply to the processing of anonymised data, other than the anonymised data referred to in section 91[316](to enable better targeting of delivery of services or formulation of evidence-based policies by the Central Government[317]).

5.2.ii. <u>Obligations of Data Fiduciary</u>

Chapter 2 of the PDP Bill provides for obligations of Data Fiduciary[318]. It stipulates that no personal data can be processed except for clear and lawful purpose[319] and requires persons processing personal data to do it in a fair and reasonable manner ensuring the privacy of the data principal[320]. Section 6 of the Bill states that 'personal data shall be collected only to the extent that is necessary for the purposes of processing of such personal data'. The Bill also provides that the data fiduciary shall give notice to the data subject about the data collected and such notice shall include the purpose and nature of data collected[321]. The Bill also limits the retention of personal data beyond the period necessary for the purpose it is processed[322] and makes the data fiduciary accountable for complying with the provisions of the Bill[323]. Sec 11

[313] Sec 2 (A) (a)

[314] Sec 2 (A) (b)

[315] Sec 2 (A) (c)

[316] Sec 2 (B)

[317] Sec 91 (2)

[318] Sec 3(13) defines 'data fiduciary' - means any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data;

[319] Sec 4

[320] Sec 5

[321] Sec 7

[322] Sec 9

[323] Sec 10

of the Bill provides for consent in processing in data[324] and states that in order for the consent to be valid it should be free[325], informed[326], specific[327], clear[328] and capable of being withdrawn[329].

The Bill also states certain exception to the general rule of consent. In the following circumstances the data fiduciary can process the data without consent (i) if required by the State for providing benefits to the individual[330], (ii) if stipulated by any Law[331] (iii) legal proceedings,[332] (iv) to respond to a medical emergency[333], (v) employment related[334], (vi) necessary for reasonable purposes[335] such as prevention of fraud, mergers and acquisitions, recovery of debt etc.

The data fiduciary must also observe specific security procedures, such as de-identification and encryption, as well as steps to ensure the integrity of personal data and prevent misuse, unauthorised access, alteration, disclosure, or destruction of personal data. [336] The Data Fiduciary is also required to report to the Data Protection Authority by notice any breach[337] of personal data.[338] Every data fiduciary is required to have the procedure and effective mechanisms to redress the grievances of data principals.[339] The 'significant data fiduciaries'[340]

---

[324] Sec 11 (1)

[325] Sec 11 (2)(a)

[326] Sec 11 (2)(b)

[327] Sec 11 (2)(c)

[328] Sec 11 (2)(d)

[329] Sec 11 (2)(e)

[330] Sec 12 (a)

[331] Sec 12 (b)

[332] Sec 12 (c)

[333] Sec 12 (d)

[334] Sec 13

[335] Sec 14

[336] Sec 24

[337] Sec 3 (*29*) "personal data breach" means any unauthorised or accidental disclosure, acquisition, sharing, use, alteration, destruction of or loss of access to, personal data that compromises the confidentiality, integrity or availability of personal data to a data principal;

[338] Sec 25

[339] Sec 32

[340]Sec 3 (*37*) "significant data fiduciary" means a data fiduciary classified as such under

have further obligations to follow. They have to carry on a data impact assessment[341], maintain records[342], shall have its policies and the conduct of its processing of personal data audited annually by an independent data auditor[343] and appoint a data protection officer[344].

5.2.iii. Rights of the Data Principal.

Chapter 5 of the PDP Bill states about the following rights of the data principal.

i) Right to confirmation and access- the data principal has the right to obtain from the fiduciary confirmation whether the personal data of the principal is processed.[345]

ii) Right to correction and erasure of personal data[346] - The data principal has the right to (a) the correction of inaccurate or misleading personal data;
(b) the completion of incomplete personal data;
(c) the updating of personal data that is out-of-date; and
(d) the erasure of personal data which is no longer necessary for the purpose for which it was processed.

iii) Right to data portability[347]

iv) Right to be forgotten- The data principal has the right to restrict or prevent the continuing disclosure of his personal data by a data fiduciary where such disclosure (a) has served the purpose for which it was collected or is no longer necessary for the purpose;

---

sub-section (*1*) of section 26;

26. (*1*) The Authority shall, having regard to the following factors, notify any data fiduciary or class of data fiduciary as significant data fiduciary, namely:—
(*a*) volume of personal data processed;
(*b*) sensitivity of personal data processed;
(*c*) turnover of the data fiduciary;
(*d*) risk of harm by processing by the data fiduciary;
(*e*) use of new technologies for processing; and
(*f*) any other factor causing harm from such processing.
(*2*) The data fiduciary or class of data fiduciary referred to in sub-section (*1*) shall register itself with the Authority in such manner as may be specified by regulations.

[341] Sec 27

[342] Sec 28

[343] Sec 29

[344] Sec 30

[345] Sec 17

[346] Sec 18

[347] Sec 19

(b) was made with the consent of the data principal and such consent has since been withdrawn; or

(c) was made contrary to the provisions of this Act or any other law for the time being in force.[348]

- The PDP Bill provides for data localisation requiring businesses to store certain categories of date only in Indian servers. In this regard, it establishes a three-tiered structure as follows: –
    1. **Personal data[349]:** Personal data that is not designated "sensitive" or "critical" is not subject to localization or data transfer limitations. No transfer limitations would apply if this type of personal data was stored wholly outside of India.
    2. **Sensitive personal data:** "sensitive personal data' may be transferred outside of India, but such data shall continue to be stored in India.[350] Sensitive personal data includes "special categories of personal data" including data relating to health, religion, sex life, political beliefs, biometric, genetic, finance etc.[351]
    3. **Critical personal data:** The bill allows the government to designate certain personal data as "essential personal data" that cannot be exported outside of India. However, the Bill allows transfers to nations or organisations that are assessed to provide an appropriate level of protection (and will not jeopardise the State's security or strategic interests).[352]

---

[348] Sec 20

[349] Sec 3 (28) of the Personal Data Protection Bill

[350] Sec 33

[351] Sec 3(36)- sensitive personal data" means such personal data, which may, reveal, be related to, or constitute—
(*i*) financial data;
(*ii*) health data;
(*iii*) official identifier;
(*iv*) sex life;
(*v*) sexual orientation;
(*vi*) biometric data;
(*vii*) genetic data;
(*viii*) transgender status;
(*ix*) intersex status;
(*x*) caste or tribe;
(*xi*) religious or political belief or affiliation; or
(*xii*) any other data categorised as sensitive personal data under section 15.

[352] Sec 34 (2)

5.2.iv. Exemptions

Chapter 8 of the Bill States about certain exemptions. The Bill empowers the Central government to exempt any agency of the government from the application of the Act in the interest of sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order; or (ii) for preventing incitement to the commission of any cognizable offence relating to sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order.[353] Exemptions are also provided on the grounds of research[354], journalistic purposes, legal proceedings, small entities[355] etc.

The Central Government has the authority to order any data fiduciary or data processor to produce anonymized personal data or other non-personal data in order to improve the targeting of service delivery or the creation of evidence-based policy.[356]

5.2.v. Data Protection Authority

Chapter 9 of the Bill lay down for the establishment of Data Protection Authority of India.[357] The Authority is mandated to ensure the compliance of the Act [358] and is given various powers for that purpose.

5.2.vi. Penalties and Compensation

Chapter 10 of the Bill stipulates penalties[359] and compensation[360] for contravening the provisions of the Act. Sec 62 of the Bill provides for the appointment of adjudicating officer for the purpose of deciding the penalties and compensation under this Chapter. The data

[353] Sec 35

[354] Sec 38

[355] Sec 39

[356] Sec 91 (2)

[357] Sec 41

[358] Sec 49

[359] Secs 57-61

[360] Sec 64

principal whose right is violated can seek for compensation[361] by making a complaint to the Adjudicating Officer.[362]

5.3. CRITICAL ANALYSIS OF THE DATA PROTECTION BILL, 2019

The Personal Data Protection (PDP) Bill, 2019, has aroused a wide spectrum of reactions, from positive to negative. Despite being hailed by some as progressive in terms of user rights and data privacy, the bill takes away with one hand what it appears to be gifting with the other.[363] This ruse is carried out by ostensibly giving a picture of a healthy user privacy framework, but it is ultimately trumped by the government's wide range of exemptions when it comes to accessing user data. Despite the bill's linguistic presentation as one that appears to prioritise users and their data, much of the bill, in the end, is concerned with how the Indian government presents itself in relation to the processing of user data by corporations and itself.[364]

5.3.i. Issues with the consent-based model

The operation of notice and consent on the internet today is flawed, according to a preponderance of evidence.[365] Consent forms are typically complicated and puzzling. As a result, people do not read them; even if they do, they may not comprehend them; and even if they comprehend, there are no procedures for giving meaningful permission in a granular manner.[366] Any enumeration of a consent framework must be built on this crucial realisation: consent does not work on the internet today.[367] The Expert Committee Report and the Bill

[361] 64. (*1*) Any data principal who has suffered harm as a result of any violation of any provision under this Act or the rules or regulations made thereunder, by a data fiduciary or a data processor, shall have the right to seek compensation from the data fiduciary or the data processor, as the case may be.

[362] Sec 64 (2)

[363] Padmini Ray Murray & Paul Anthony, *Designing for Democracy: Does the Personal Data Protection Bill 2019 Champion Citizen Rights?* Vol. 55:21 Economic and Political Weekly, (2020)

[364] Id

[365] Ryan M. Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87: 3 Notre Dame Law Review at 1031; (2012)

[366]Bart Schermer, Bart Custers, and Simone van der Hof, "The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection," 16:2, *Ethics and Information Technology* 19 (2014) https://link.springer.com/article/10.1007/s10676-014-9343-8.

[367] A free and fair digital economy, protecting privacy, empowering Indians, Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, Pg-114, https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf (last visited 27/08/2021, 7:00 am)

admit that users are incapable of giving meaningful consent, yet they build on the idea that greater consent mechanisms can lead to better outcomes, which is somewhat paradoxical.
According to an IBM survey, even while people believe corporations should be more severely regulated for data management, 71% were prepared to give up privacy in exchange for access to the technology they want, and only 16% had ever left a company due to data misuse.[368] Should a legal framework impose a consent-based regime if consumers do not employ consent agreements to preserve their online privacy, especially in the absence of clear proof that it will work?- is a confusing question.

Furthermore, a consent-based approach may exacerbate current problems. According to one article, a consent-and-notice approach modelled after the EU's GDPR (as the bill is) is likely to worsen the cognitive difficulties associated with granting meaningful consent.[369] Users must struggle with an overflow, not a lack, of disclosure-related information concerning consent under existing frameworks, according to the Srikrishna committee.[370] If present consent methods result in information and consent overload, the bill's proposal for "stronger" consent is likely to worsen these problems. As a result, the proposed framework would provide consumers with more information (permission agreements would have to include additional disclosures, rights, and obligations, and new consent would be required for each new purpose), without necessarily compromising data privacy.
Moreover, the existence of harsh penalties in the GDPR for failing to comply with notice and consent requirements has been criticised on the grounds that it is likely to make technology companies more risk-averse, resulting in consent agreements with stronger opt-in clauses and a more legalistic tone[371]. Violations would be subject to harsh monetary penalties, according to the measure.[372] Users and businesses may suffer as a result of this. Increased consent requirements may cause users to become less receptive to consent agreements. Firms, on the other hand, may find that users have less trust in them if they believe they have been deceived, even though the firm has followed all legal obligations.[373]

[368] Erik Sherman, "People Are Concerned About Their Privacy in Theory, Not Practice, Says New Study," *Fortune*, February 25, 2019, https://fortune.com/2019/02/25/consumers-data-privacy/.
[369] Schermer, et al.,supra note 366.
[370] Supra note 367 at 32.
[371] Schermer, et al, *supra* note 366
[372] Sections 57-59 of the bill.
[373] Schermer, et al.,supra note 366.

A professor of information technology and public policy, Alessandro Acquisti, points out that relying too heavily on consent has its own set of costs that could jeopardise data protection goals. He writes:

"Additional costs . . . comprise the social losses due to 'incoherent privacy policies': amidst a complex array of legislative and self-regulatory initiatives, both consumers and firms are uncertain about the level of protection afforded to, or required for, various types of personal data. This uncertainty is costly in itself, in that it forces data subjects and data holders to invest resources into learning about the admissibility of a given data practice. It also creates costly second order effects, in that it may lead both data subjects and data holders to inefficiently under- or over-invest in data protection"[374]

As a result, the proposed notice-and-consent structure could be counterproductive. It's possible that it won't genuinely eliminate internet damages, but will instead worsen moral hazard. Users may become more reliant on regulation and less cautious in their online activities. Additionally, users' cognitive burdens may increase. As a result, consent rules may become pointless in terms of protecting personal data. If the proposed notice-and-consent framework fails to meet its claimed goal of adopting a preventive privacy framework, the costs will outweigh the advantages for a country like India.[375]

5.3.ii. Wide powers to the Central Government

"The PDP Bill has been used by the government as yet another opportunity to flex its paternalistic muscle: there is much made of its quest for protectionist strategy of data sovereignty against the continued onslaught of data colonialism enacted by foreign technology corporations such as Facebook and Google."[376] The Justice Srikrishna committee has rightly pointed out that, 'A data protection law, to be meaningful should, in principle, apply to the State. It would indeed be odd if a law enacted to give effect to a fundamental right to privacy does not serve to protect persons from privacy harms caused by processing of personal data by the State'[377]. The Expert Committee's proposed Legislation[378] allowed for exemptions in the

[374] Alessandro Acquisti, "The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines," in *Joint WPISP-WPIE Roundtable* (OECD, 2010), https://www.oecd.org/sti/ieconomy/46968784.pdf, 14.

[375] Anirudh Burman, Will India's Data Protection Law Protect Privacy and Promote Growth?, March 2020, https://carnegieendowment.org/files/Burman_Data_Privacy.pdf, 17

[376] Murray and Anthony, Supra note 363

[377] Supra note 367 at 32.

[378] Data Protection Bill, 2018

interests of national security when sanctioned by a law enacted by Parliament, as long as the exemption complied with globally recognised standards of necessity and proportionality. In contrast, under Section 35[379] of the PDP Bill 2019, a single executive order from the Central Government authorising any government agency to process personal data can allow them to conduct surveillance without any explicit safeguards. It allows the central government to exempt "any" government entity from "all or any" of the act's provisions for the processing of specific personal data. The government can also take such action if it believes it is "necessary or expedient" in the interests of India's sovereignty and integrity, security, friendly relations with foreign countries, and public order. Furthermore, the government may be granted an exemption for the purpose of preventing incitement to commit any cognizable offence relating to India's sovereignty and integrity, security, cordial relations with foreign nations, and public order. Section 35 differs significantly from the Justice Srikrishna Committee's earlier version of the Personal Data Protection Bill- 2018, which simply exempted data processing "in the interests of the state's security." When the Expert Committee advised that such exemptions be created solely through legislation, the above-mentioned change should be viewed as a purposeful attempt to weaken the right to privacy.

“Section 35 of the Data Protection Bill considerably eases the government’s task of collecting data to compulsorily register its citizens, which flagrantly disregards the scope allowed by the Puttaswamy judgment, which only allowed “necessary and proportionate” processing of data by the government under a limited number of conditions. In addition to this, the emphasis on data localisation allows the government to collect data on transactions that ordinarily would have been processed outside the country before the Bill was tabled.”[380]

The PDP Bill mandates the government's sharing of non-personal data that has been obtained and generated privately. The Government may direct any data fiduciary or data processor to disclose any personal data anonymized or other non-personal data to enable improved targeting of service delivery or formulation of evidence-based policies by the Central Government, according to Section 91(2) of the Bill. To begin with, it is incomprehensible why a personal data protection regulation would deal with non-personal data at all. Second, this provision

[379] Sec 35- Power of Central Government to exempt any agency of Government from application of Act.

[380] Murray and Anthony, Supra note 363

makes no mention of how the government will utilise such data or if enterprises that are required to share such data will be reimbursed. As a result, the Central Government has the right to expropriate intellectual property under this provision, which is likely to have long-term negative consequences for innovation incentives.[381]

As per Section 14[382] of the PDP Bill, the Government can process personal data without consent for some "reasonable purposes" which include whistleblowing. The provision also gives the government the authority to evaluate whether or not the obligation of notice to the data principal is necessary through regulations. Whistleblowers who uncover scams or irregularities may be subjected to systematic harassment as a result of this.[383]

5.3.iii. Limited Powers of the Data Protection Authority

In comparison to the last version of the Personal Data Protection Bill, 2018, written by a Committee of Experts led by Justice Srikrishna, we see an abrogation of powers in this Bill for the Data Protection Authority.[384] The Authority's initial powers and functions are now vested with the Central Government. Consider the following scenario: (i) The Authority was given the authority in the 2018 Bill to notify additional types of sensitive personal data. The power to do so has been given to the Central Government in cooperation with sectoral regulators under the current Bill. (ii) Under the 2018 Bill, the Authority had sole authority to determine and notify significant data fiduciaries; however, under the current Bill, the Central Government has been given the authority to notify social media intermediaries as significant data fiduciaries after consultation with the Authority.[385]

The PDP Bill, in its current form, appears to be magnanimous when it comes to user rights or the data principle (as users are characterised in the bill). The first bill to directly address user privacy, it appears to match itself with some elements of the European Union's (EU) General Data Protection Regulation (GDPR) model, allowing for rights to portability, explainability, and object to data processing, as well as solutions derived from such processing. The bill establishes the Data Protection Authority (DPA), which, on paper, protects the rights of data

[381] Renjith Mathew, *Personal Data Protection Bill, 2019 –Examined through the Prism of Fundamental Right to Privacy – A Critical Study*, (22 May 2020,) https://www.scconline.com/blog/post/2020/05/22/personal-data-protection-bill-2019-examined-through-the-prism-of-fundamental-right-to-privacy-a-critical-study/#_ftn26

[Accessed 7 July 2021].

[382] Sec 14. Processing of personal data for other reasonable purposes.

[383] Mathew, supra note 381

[384] Mathew, supra note 381

[385] Mathew, supra note 381

principals by questioning data fiduciaries, who include both commercial enterprises and the government. The right to explainability permits the DPA to educate data subjects about how their data is being used, which is made possible by a suggested method known as the consent manager, which is a portal that allows data subjects to view how their data is being used and how it is being used.

However, the DPA's ostensibly generous creation in the interests of citizens is already jeopardised by the proposed composition of the DPA itself; unlike the previous version of the bill, which included the chief justice in the line-up, the selection committee to elect the DPA's members has no representation from the judiciary. It's difficult to tell how representative the DPA will be of citizen and consumer rights in its current form, and this lack of clarity may not be intentionally.

5.3.iv. Non-compliance with Puttaswamy[386] ruling

The 2018 bill exempted the processing of personal data if it met four criteria: first, it was authorised by law; second, it was carried out in accordance with the procedure established by such law, enacted by Parliament; third, it was necessary to achieve such goals; and fourth, it was proportionate in its application. These rules were put in place in response to the Supreme Court's decision in the historic Justice K.S. Puttaswamy vs. Union of India (Right to Privacy) case. Indians have a constitutionally guaranteed fundamental right to privacy, according to the unanimous verdict. The decision also stated that any exemption from the act's application should be narrowly circumscribed. Even back then, the 2018 bill was criticised for essentially giving the government carte blanche.[387]

There could be instances of national security, defence etc which might need expedient actions that could even infringe the privacy rights of people. It could be the reasons for the Bill granting powers to the Central Government to process personal data under Sec 35 of the Bill. While national interests may supersede individual private interests in some situations, as the Justice Srikrishna Committee found, it is vital, "to ensure that the pillars of the data protection framework are not shaken by a vague and nebulous national security exception."[388]

---

[386] (2017) 10 SCC 1

[387] *New data bill gives sweeping powers to govt*. https://www.telegraphindia.com/opinion/new-data-bill-gives-sweeping-powers-to-govt/cid/1726583 (Accessed 20 September 2021).

[388] Burman, Supra note 375

The 2019 bill, on the other hand, eliminates these safeguards entirely, replacing them with a simple requirement that the central government issue an order, documenting its reasons in writing, and subject to "such procedures, safeguards, and oversight mechanism to be followed by the agency as may be established". As a result, the government has delegated the crucial duty of oversight and accountability to regulations that will be directly announced by the Data Protection Authority — and hence will not be debated in Parliament — and will almost certainly lack judicial scrutiny.[389] The Bill's broad powers provide the government the ability to conduct widespread surveillance, which violates the fundamental right to privacy. As a result, the PDP Bill fails to qualify the Puttaswamy judgment's standards for identifying violations of the fundamental right to privacy in more than one way.[390]

- The most recent measure proposes the formation of a distinct class of key "data fiduciaries" known as "social media intermediaries" in order to govern social media businesses, which is a break from both the GDPR and the 2018 iteration of the bill. These are entities whose major function is to facilitate online connection amongst people (and does not include intermediaries that enable business transactions or access to the internet, or that are in the nature of search engines or encyclopedias). A "data fiduciary" is essentially a social media corporation. The bill contains ambiguous language that states that social media intermediaries must allow voluntary account verification by any users who use their services or register from India. However, it is unclear what documentation users must provide to the social media intermediary in order to validate their accounts. This type of voluntary verification procedure is not available in any other country.[391]

[389] Supra note 387

[390] Mathew, supra note 381

[391] Basu, A. and Sherman, J., *Key Global Takeaways From India's Revised Personal Data Protection Bill*. Lawfare. (Accessed 23 September 2021). <https://www.lawfareblog.com/key-global-takeaways-indias-revised-personal-data-protection-bill

5.4. CONCLUSION

The new Personal Data Protection Bill of 2019 is a step in the right direction toward enacting a data protection and privacy law that applies to all Indians. It strengthens the existing notice and consent framework by introducing concepts of collection limitation, data retention, and purpose limitation. At the same time, the bill significantly expands the government's exclusions from these and other data protection standards, raising serious concerns about citizens' privacy.[392]

The proposal of a data protection measure in support of a constitutionally protected right to privacy is a minor step toward taking the lead on democratic data governance. The bill's wording, on the other hand, looks to be a mash-up of GDPR rules with authoritarian overtones. These include the bill's enabling structure for government monitoring, which unquestionably entrenches government power to violate citizen privacy. In addition, the blurring of the lines between non-personal and personal data is troubling. In the end, the bill weakens individual data privacy protections by allowing the government to access whatever it deems to fall under the defined categories of exemptions.

India's ability to advise rising market economies and smaller democratic republics is harmed by its authoritarian tendencies. The bill makes India a less enticing model for countries seeking to develop a new vision of data governance that incorporates both the right to privacy and essential civil liberties. Though the bill contains some privacy-protecting elements that are similar to those found in the GDPR, it need considerable adjustments if India is to be a leader in developing a democratic, privacy-protecting approach to the internet. Consultative processes that prioritise how technology is used and experienced must be put in place for this bill to fully represent citizens, whether they are located at the last mile or at the cutting edge, or it risks becoming a document that only guarantees the rights of its constituents on paper.

India's strategic goal is likely to be in ensuring that it fulfils its constitutional commitment to its people, prioritising citizen rights and economic well-being over purely commercial or bureaucratic concerns. However, it is unclear whether this goal is met, owing to concerns about exemptions in the language of the Personal Data Protection Bill. It remains to be seen whether the policymaking pendulum swings in the appropriate direction as the Joint Parliamentary Committee begins debates on the bill draught.

[392] Supra note 387

CHAPTER 6

CONCLUSION AND SUGGESTIONS

"The titanic power struggles of the twentieth century were between industrial capital and labor, but the twenty-first century finds surveillance capital pitted against the entirety of our societies in a bloodless battle for power and profit as violent as any the world has seen. Let there be a digital future, but let it be a human future first" – Shoshana Zuboff'[393]

6.1. SYNOPSIS OF CONCLUSIONS

This study intended to analyse the efficiency of data protection laws in India. The research agenda, scope and limitations were presented in the first chapter. The Second chapter traces the origin and development of the concept of privacy and the right to privacy in India. Various international legal documents, cases from various jurisdictions, position of Indian judiciary were analysed. In India, the right to privacy is now a fundamental right. The third chapter examined the evolution of data privacy and its nuances. It also focused on right to erasure and right to be forgotten which are aspects of data privacy in detail. The chapter four assessed data protection laws in Australia, USA and UK. Chapter five critically examined the draft Data Protection Bill, 2019 to pinpoint its flaws and suggest changes. It was found that with excessive powers granted to the Central Government to intervene in individual privacy without taking an actual recourse to 'procedure established by law' has a 'chilling effect' to right to privacy in India. This chapter concludes by stating the findings of the study and by making recommendations for a robust data protection regime in India.

Economic progress necessitates data-driven innovation. But how much will it cost? We are easily convinced as a society to give up our privacy in order to use apps that follow our every move. It's practically impossible to opt out. In an ideal world, privacy regulations would totally

[393] https://shoshanazuboff.com/book/about/,(last visited on 22/09/2021, 11:00 am)

safeguard customers with minimal bargaining power while also assisting the economy's growth.

The more digitalised our lives have become; the more is the chance for privacy infringement with or without our knowledge many a time. There are a lot of challenges that the world face due to the emergence of various social media applications and devices governed by artificial intelligence. These challenges will grow in the future as the technological advancement and introduction of new applications happen more often than usual.

The main challenges at hand for the data protection regime to handle are

- The volunteered data

  "The ubiquity of 'volunteered' data notably through the development in wearable devices and social media networks, is the first obstacle to defending the right to data protection today, even if users of such devices may not think of themselves as offering data to others (Lyon, 2014). The rise of the so-called "quantified self," or the self-tracking of biological, environmental, physical, or behavioural information through tracking devices, Internet-of-things devices, social network data, and other means (Swan, 2013), may result in data being gathered not only about the individual user, but also about people around them. As a result, relying exclusively on consent to protect one's data is insufficient, especially when data obtained for one purpose can be repurposed for another."[394]

- Profiling

  Data subjects are frequently ignorant of the amount and type of information collected about them, as well as how this information might be linked to infer their traits using artificial intelligence technologies. Users have no knowledge of or control over their classification or how interconnected systems treat them depending on this categorization, which is a major risk of this form of profiling. According to research, such targeting of information can lead to individuals gaining excessive confidence in their points of view, which can lead to extremism and polarisation in society. Future data protection and privacy research should concentrate on potential solutions to this dilemma.

- Conditioning

  It is anticipated that in the same way that industrial capitalism ruined the natural world in the twentieth century, a worldwide architecture of behaviour modification threatens human nature

[394] McDermott, *supra* note 79

in the twenty-first. The Artificial Intelligence related technologies could modify our behaviour and condition us to the need of the capitalists.

- Surveillance Capitalism

Soshanna Zuboff in her book 'The Age of Surveillance Capitalism: The fight for a Human Future at the New Frontier of Power'[395] discusses about surveillance capitalism- a business model that underpins the digital world. This necessitates a new form of capitalism, one that runs by delivering "free services" to billions of people, allowing providers to track their customers' activity in incredible detail, often without their explicit agreement. "Unilaterally, surveillance capitalism claims human experience as free raw material for translation into behavioural data," writes Zuboff, "Although part of this information is used to improve service, the rest is classified as a private behavioural surplus that is fed into advanced manufacturing processes known as "machine intelligence" and turned into prediction products that predict what you will do now, soon, and later. Finally, these prediction products are sold in behavioural futures markets, which are a new type of marketplace. Surveillance capitalists have become extremely wealthy as a result of these trading operations, as many firms are willing to stake their future on our actions."

6.2.Consent Based Model

Most of the data protection laws across the globe are 'consent based'. The proposed data protection Bill and the GDPR is based on the 'consent model' of data protection. Once a data subject's consent has been gained, the data controller is free to collect, process, and use the data for the stated purpose and is not responsible for any consequences that may arise as a result of its actions. This puts the responsibility on the individual to be mindful of the terms of data access to which he is consenting. Data controllers definitely benefit more than data subjects as a result of this.

Since there were few reasons to acquire data and few further uses to which it might be put previously, the Consent Model sufficed. Data was static once it was acquired, and it was rarely

[395] ZUBOFF, SHOSHANA. THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (New York: PublicAffairs, 2019)

shared outside of the company. As a result, data subjects had a clear understanding of what data was being gathered and for what purposes it would be used, allowing them to make informed decisions. The Consent Model was both possible and adequate in this situation.

But now the situation has changed. Our activities online are monitored, with every search in google, like in Facebook or Instagram, tweet in twitter, online purchases made our identity is being established and are being profiled to fit into categories which we have not even heard of. We are surrounded by smart devices with sensors and cloud intelligence that track our activities. Further, there is a huge imbalance in the power the data subject and controllers hold. Unless we consent to the particular 'standard form of contract' we cannot avail the service offered by the data controller, making it mandatory for us to consent. We agree to this data collection by signing complex and long standard form of contracts that are complicated and hard to understand. This in effect weakens the position of a data subject.

6.3.Rights Model of Data Protection Law

Rights based model comes as an effective alternative to overcome the shortcomings of consent-based model. The rights model ensures that the data subject's interests are protected and the burden of ensuring data privacy is now on the data controllers distinct from the consent model. This model assures the inalienable right of individuals over their personal data. The rights based models are found on the principles of autonomy, security and accountability.

Accountability – The data controller must be responsible for the data under their control; irrespective of consent from the data subject. Autonomy- All data subjects should have autonomy over their data, where they cannot effectively prevent collection of data, they should have the option to restraint or limit the manner in which data is processed. Security- The data must be treated securely from collection, processing, use and destruction.

The rights- based model has the following implications

- Every individual has some inalienable rights over their personal data. The data controllers are obliged to ensure these rights. The data controller will have fiduciary responsibility over the data under their control and liable for any harm consequential thereto.
- The data controller has liability in case of any harms caused to the data subject. The rights-based model identifies the potential harms and finds remedies to them.

It is however, not argued that rights-based model is failproof, but it would be efficient than the consent- based approach to data protection.

6.4.Need for a Global Standard of Data Protection

"That we are now living through a new generational shift in the respect of privacy. This shift is towards establishing a sustainable ethics for a digitised society. It is driven by the globalisation of the economy and the socio-technological forces…It is driven by the digitisation of almost everything in our economy and services sector, our social relations, politics and government. Above all, it is driven by the prospect of human decision-making, responsibility and accountability being delegated to machines. Digitisation respects no geographical boundaries. It is not sensitive to human boundaries between what we want to be public, private or something in between. It injects itself into our most intimate spaces-relationships, communications and attention. The so-called 'privacy paradox' is not that people have conflicting desires to hide and to expose. The paradox is that we have not yet learned how to navigate the new possibilities and vulnerabilities opened up by raped digitisation. What do I mean by ethics? Ethics is the sense we all have, often subconscious, of right and wrong in different circumstances. Philosophical on this stage will shortly explain how ethical consensus have emerged in the past. In today's digital sphere, however, there is no such ethical consensus. We do not have a consensus in Europe and we certainly do not have one at a global level. But we urgently need one."[396]

There is an urgent need for a global consensus on data protection standards. Data protection laws varying from country to country make it hard for the companies to comply with. They are forced to change the data protection terms and policies in changing territories. The demerits of the same are twofold. One, there is no uniformity in the rights protected in various countries. Secondly, the same company would have varied privacy policies in various countries, the drafting of which is a tedious task. With the privacy requirements changing, the companies have to spend more time to update their policies which again is not uniform.

Currently GDPR is the only regulation that has got wide application. However, it cannot be considered as a global one. There should be a globally set standard for data protection to understand what are 'good data protection laws'. To provide consistent data protection among

[396] Alen Charles, supra note 226 at 3

industries and promote greater consistent data privacy compliance, a clear, realistic, and worldwide adequacy standard is required.

6.5.Data Protection in India

Since there is no proper data protection law in India, it is now regulated by the provisions of IT Act and IT Rules which will not suffice the current requirements and the rapid growth of technology. The proposed Data Protection Bill, 2019, though is the first legislation on data protection in India has many demerits as analysed in Chapter V. Hence, it could be understood that there is no adequate data protection law in India. If the present Bill is passed without adequate changes to ensure and facilitate data protection, it would remain as a missed opportunity for a profound law making that could have been basis for various data protection laws across the globe.

6.5.i. Right to Erasure and Right to be Forgotten

Under the PDP Bill, 2019 Right to correction and Erasure of personal data either changes, updates or erases the existing data, while the right to be forgotten permits the data principal to have his personal data non-disclosed. That means the data remains unchanged but it is just kept hidden or away from search engines. The right to be forgotten in India is quite different from the 'right to be forgotten' under GDPR which permits total deletion or erasure of data (however, whether something could be deleted from the internet is still dubious). The request for erasure is made to the data fiduciary who would decide on the matter while in case of Right to be forgotten it is the Adjudicating Authority who could enforce the right.

6.6. RECOMMENDATIONS AND SUGGESTIONS: -

6.6.i. National Level

- The right to data privacy should be made a constitutional one as it would impose duties on the State to respect, protect and fulfil the right for everyone , including the poor and vulnerable who may not be able to secure protection on their own.
- The Data Protection Bill 2019 should be amended so as to ensure the enforceability of its provisions even against the State.

The amendments on the Bill could be made to effectuate the following.

1. Restricting the wide powers of the Central Government.

   The PDP Bill 2019, under Sec 35 permits the Central Government to authorise any government agency to process personal data with a mere executive order. Thus, widening the 'dataveillance', without following the requirements of proportionality and necessity.

2. Strong and Independent Data Protection Authority

   The Data Protection Authority should be the main organ to decide on matters of Data Protection. The PDP Bill 2019 delegates many functions which ought to have been that of the Data Protection Authority to the Central Government. This not only increases the chance of those powers being misused for the interests of Central Government, but also diminishes the value, independence and purpose of the Data Protection Authority. The composition of the Data Protection Authority should be made more representative and outside the clutches of the legislature.

3. The Bill should be made compliant to the Puttaswamy Ruling

   The Puttaswamy judgment states some stipulations for the Government to process personal data, it necessitates that, firstly it should be authorised by law; second, it was carried out in accordance with the procedure established by such law enacted by Parliament; third, it was necessary to achieve such goals and fourth, it was proportionate in its application.

4. Rights based model should be followed

   Unlike the consent- based model upon which the PDP Bill is now based, a right based approach would be more efficient in protecting data privacy of citizens.

5. Defining 'privacy'

   The Preamble of the Bill states that protection of privacy as its objective. However, the term privacy is left undefined. Though technology is changing at an exponential rate, the values underpinning privacy remains same. Defining privacy in its truest and broadest sense in consonance with its core value would ensure that it is protected, irrespective of technical advancements.

6. Quicker means of remedy

The data principal whose rights are violated should get expedient remedy especially in terms of matters online which could be shared, copied or downloaded within seconds. The concept of 'wait it out' till the Courts have reached a conclusion will not meet the demand of the time. Therefore, effective and expedient means for remedy have to be present.

If the above suggestions are implemented, India will undoubtedly be on the way to become a data privacy compliant nation that promotes security and development of the country and people.

6.6.ii Global Level

- The right to data privacy must be recognised as a human right and the international organs must stipulate guidelines for the protection of data that could form the basis of various national legislations.
- A global consensus on the values on which the data protection laws across the globe would be ideal as data is something that transgress the boundaries and territories of nations or continents.
- The rights- based model of data protection laws could be implemented by the countries across the globe.
- There should be a limit to self-regulation in the private sector. Strong and Independent bodies for data protection should be established which could issue guidelines for the private sector entities.
- Though, the current situation necessitates cross border data flows, it should be done according to the law.

Difficult to enact, doubtful of effectiveness and with no insurance against an uncertain future, the overall suitability of information privacy laws to counter digital remembering and privacy breach are unclear. The governments across the world must pave way for digitalised future for the benefits it alone could offer, but it should not be made sabotaging the basic human right of privacy of the people.

BIBLIOGRAPHY

ARTICLES

- Adam D. Moore, *Toward Informational Privacy Rights*, 44 San DIEGO L. REV. 809 (2007).
- B. W. Schermer et al, *The crisis of consent: how stronger legal protection may lead to weaker consent in data protection,* 16(2) Ethics and Information Technology (2014)
- Benjamin Wong, The journalism exception in UK data protection law, 12:2, Journal of Media Law, 216-236, (2020)
- Bratman, *B. E.: Brandeis and Warren's The Right To Privacy and the Birth of the Right to Privacy,*69 Tennessee Law Review 344 (2002)
- Charles Fried, *Privacy*, 77 Yale L. J., Vol.77, 475 (1968)
- Christina P. Moniodis, *Moving from Nixon to NASA: Privacy 's Second Strand- A Right to Informational Privacy,* 15:1Yale Journal of Law and Technology 154, (2012)
- DeVries W, *Protecting privacy in the digital age,* 18 Berkeley Tech LJ 283–311(2003)
- Diane P. Michelfelder, *The moral value of informational privacy in cyberspace,* 3 Ethics and Information Technology 129–135, (2001)
- Edward Lee, "The Right to be Forgotten v. Free Speech" Journal of Law and Policy for the Information Society, 103 (2015)
- Felicia Lamport, "DEPRIVACY", Look Magazine, 1970.
- George B. Trubow, *Protecting Informational Privacy in the Information Society*, 10 N. ILL. U. L. REV. 521 (1990).
- Helscher D, *Griswold v. Connecticut and the unenumerated right of privacy,* 15 N Ill U L Rev 33–61 (1994)
- James Madison, *Essay on Property*, in Gaillard Hunt ed., 6 The Writings of James Madison 101-103, (1906).
- Laura Bradford, Mateo Aboy, Kathleen Liddell, *A Stress Test for Privacy, the GDPR and Data Protection Regimes,* Journal of Law and Biosciences, 25 (2020)
- McGeveran W, *Friending the privacy regulators*. 58 Arizona Law Review. 959-961, (2016)

- Michael C. James, *A Comparative Analysis of the Right to Privacy in the United States, Canada and Europe*, 29:2, Connecticut Journal of International Law, *261* (Spring 2014),
- Mike Wagner & Yun Li-Reilly, *The Right to be Forgotten*, 72:6 The Advocate, Nov. 2014
- Moira Paterson & Maeve McDonagh, *Data Protection in an Era of Big Data: The Challenges Posed by Big Personal Data*, 44 Monash University Law Review 1 (2018).
- Nishant Shah, *Identity and Identification: The Individual in the Time of Networked Governance*, 11 Socio-LEGAL REV. 22 (2015).
- Nuala O'Connor, Alethea Lange and Ali Lange, *Privacy in the Digital Age,* Great Decisions, 19, 17-28(2015),
- Padmini Ray Murray & Paul Anthony, *Designing for Democracy: Does the Personal Data Protection Bill 2019 Champion Citizen Rights?* Vol. 55:21 Economic and Political Weekly, (2020)
- Prosser, W.: *Privacy, 48:3* California Law Review, 384 (1960)
- Reidenberg J, *Resolving conflicting international data privacy rules in cyberspace*, 52 Stan L Rev 1315–1371 (2000)
- Richard A. Posner, *Privacy, Surveillance, and Law, 75* University of Chicago Law Review 245 (2008)
- Schwartz P, Solove D, *Reconciling personal information in the United States and European Union*, 102 Calif L Rev 877–916 (2014)
- Solove D, Hartzog W, *The FTC and the new common law of privacy*, 114 Colum L Rev 583–676 (2014)
- Terry N, *Existential challenges for health care data protection in the United States*, 3 Ethics Med Public Health 19 (2017)
- Warren and Brandeis, *The Right to Privacy,* 5 Harvard Law Review, 193 (1890),
- Weber, Rolf H. *"The right to be forgotten." More than a Pandora's Box,* 2 Journal of Intellectual Property, Information Technology and E-commerce,120-130 (2011)
- Yvonne McDermott, *Conceptualizing the right to data protection in an era of Big Data*, Big Data and Society 1, (2017)

BOOKS

- ALEN CHARLES RAUL, THE PRIVACY, DATA PROTECTION AND CYBER SECURITY LAW REVIEW, 374 (The Law Reviews, 2019)
- ARTHUR R. MILLER, THE ASSAULT ON PRIVACY, 39 (Ann Arbour, Michigan University Press, 1971)
- DANIEL J SOLOVE, THE DIGITAL PERSON, 26 (New York university Press, 2004).
- DARIO MAURA VINCETE & SOFIA DE VASCONSELS, DATA PROTECTION IN THE INTERNET, 412 (Springer 2020)
- ELIF KIESOW CORTEZ, DATA PROTECTION AROUND THE WORLD-PRIVACY LAWS IN ACTION, 232 DARIO MAURA VINCETE & SOFIA DE VASCONSELS, DATA PROTECTION IN THE INTERNET, 412 (Springer 2020)
- HANNAH YEEFEN LIM, DATA PROTECTION IN THE PRACTICAL CONTEXT, 12 (Academy Publishing, 2017)
- HOOFNAGLE C, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY, (Cambridge University Press, New York , 2016)
- JAMES WALDO, HERBERT S. LIN, LYNETTE I. MILLETT, ENGAGING PRIVACY AND INFORMATION IN A DIGITAL AGE 48 (The Academies Press, 2007)
- JOHN STUART MILL, ON LIBERTY, 13, (Batoche Books 1859),
- MARK BURDON, DIGITAL DATA COLLECTION AND INFORMATION PRIVACY LAW 2 (Cambridge University Press, 2020)
- MARK BURDON, DIGITAL DATA COLLECTION AND INFORMATION PRIVACY LAW, (Cambridge University Press, 2020)
- NEIL RICHARDS, INTELLECTUAL PRIVACY-RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE, 104 (Oxford University Press, 2015)
- SWIRE P AND AHMAD K, FOUNDATIONS OF INFORMATION PRIVACY AND DATA PROTECTION: A SURVEY OF GLOBAL CONCEPTS, LAWS AND PRACTICES. (International Association of Privacy Professionals, Portsmouth, 2012)

- VIKTOR MAYER SCHONBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE, (Princeton University Press, 2009)
- WILLIAM W. LOWRANCE, PRIVACY, CONFIDENTIALITY AND HEALTH RESEARCH 7 (Cambridge University Press, 2012).
- ZUBOFF, SHOSHANA. THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (New York: PublicAffairs, 2019)

CONVENTIONS

- African Charter of Human and People's Rights, 1981
- African Charter on the Rights and Welfare of the Child, 1990
- American Convention on Human Rights ,1967
- American Convention on Human Rights, 1969
- Convention on the Rights of Child, 1989
- Convention on the Rights of Persons with Disabilities, 2007
- European Convention on Human Rights (ECHR), 1950
- International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, 1990
- International Covenant on Civil and Political Rights (ICCPR), 1966

STATUTES AND BILLS

- California Consumer Privacy Act, 2020
- Children's Online Privacy Protection Act, 1998
- Computer Fraud and Abuse Act, 1986
- Constitution of India, 1950
- Controlling the Assault of Non-Solicited Pornography and Marketing Act, 2003
- Data Protection Act of 2018
- Electronic Communications Privacy Act, 1986
- European Convention on Human Rights (ECHR), 1950

- Family Education Rights and Privacy Act, 1974
- General Data Protection Regulation, 2018
- Gramm-Leach- Bliley Act, 1999
- Health Insurance Portability and Accountability Act (HIPAA), 1996
- Information Technology Act, 2000
- Personal Data Protection Bill, 2019
- Privacy Act 1988
- The Fair Credit Reporting Act, 1970

ONLINE SOURCES

- "CAN-SPAM Act: A Compliance Guide for Business", Federal Trade Commission. Available at: https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guidebusiness. (last visited on 25/08/2021, 10:00 am)
- A free and fair digital economy, protecting privacy, empowering Indians, Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, Pg-114, https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf (last visited 27/08/2021, 7:00 am)
- ACCC, Digital Platforms Inquiry, Final Report, June 2019, Page 462, https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf
- African Charter on the Rights and Welfare of the Child, https://au.int/sites/default/files/treaties/36804-treaty-african_charter_on_rights_welfare_of_the_child.pdf, (last accessed 4/10/2021, 7:00 am)
- Alessandro Acquisti, "The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines," in *Joint WPISP-WPIE Roundtable* (OECD, 2010), https://www.oecd.org/sti/ieconomy/46968784.pdf, 14.
- Allens, *In a nutshell: data protection, privacy and cybersecurity in Australia*, Lexology, (October 2020) https://www.lexology.com/library/detail.aspx?g=2027ba56-6178-4e7f-9273-9aa9bb2f5066

- Amber Sinha, *Right to be Forgotten – A Tale of two Judgments*, Centre for Internet Society, (last accessed on 18/04/2021) https://cis-india.org/internet-governance/blog/right-to-be-forgotten-a-tale-of-two-judgments
- Anirudh Burman, Will India's Data Protection Law Protect Privacy and Promote Growth?, March 2020, https://carnegieendowment.org/files/Burman_Data_Privacy.pdf, 17
- Asha Barbaschow, *Australian privacy law amendments to cover data collection and use by digital platforms*, (last visited on 24/08/2021, 11:30 am) https://www.zdnet.com/article/australian-privacy-law-amendment-to-cover-data-collection-and-use-by-digital-platforms/
- Australian Government- Federal Register of Legislation, https://www.legislation.gov.au/Details/C2021C00242, (last visited on 22/08/2021 10:30 am)
- Bart Schermer, Bart Custers, and Simone van der Hof, "The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection," *Ethics and Information Technology* 16, no. 2 (2014): 19, https://link.springer.com/article/10.1007/s10676-014-9343-8.
- Basu, A. and Sherman, J., *Key Global Takeaways From India's Revised Personal Data Protection Bill*. Lawfare. (Accessed 23 September 2021). https://www.lawfareblog.com/key-global-takeaways-indias-revised-personal-data-protection-bill
- Bhandari, V., Kak, A., Parsheera, S., & Rahman, F., *An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict* (accessed on 25/08/2021, 5:20 pm) https://www.indrastra.com/2017/11/An-Analysis-of-Puttaswamy-Supreme-Court-s-Privacy-Verdict-003-11-2017-0004.html
- *Big Data: Seizing Opportunities and Preserving Values*, Executive Office of the President, May 2014, https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf accessed on 10/07/2021, 14:30 pm.

- Cathy O Neil, *Big Data Algorithms are Manipulating Us*, WIRED, (accessed on 29-06-2021- 10:31 am) all-https://www.wired.com/2016/10/big-data-algorithms-manipulating-us/-
- David Watts and Pompeu Casanovas, *Privacy and Data Protection in Australia: a Critical overview (extended abstract),*(visited on 25/08/2021) https://www.w3.org/2018/vocabws/papers/watts-casanovas.pdf
- Directive 95/46/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046 (last visited on 6/10/2021, 10:30 pm)
- Doyle C (2012) *Privacy: an overview of the Electronic Communications Privacy Act.* Congressional Research Service, https://www.hsdl.org/?view&did¼725508
- Dr. Jasmine Alex,*Privacy In Cyber Space*., Livelaw, (Accessed 3 February 2021) https://www.livelaw.in/columns/privacy-in-cyber-space-157769
- Erik Sherman, "People Are Concerned About Their Privacy in Theory, Not Practice, Says New Study," *Fortune*, February 25, 2019, https://fortune.com/2019/02/25/consumers-data-privacy/.
- https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf
- J.Steven Perry, What is Big Data? More than Volume, Velocity and Variety...IBM Developer Blog (2017). https://developer.ibm.com/blogs/what-is-big-data-more-than-volume-velocity-and-variety/, (last accessed on 06/7/2021- 6:53 am.)
- Jeffrey Rosen, *The Right to be Forgotten*, Symposium Issue, 64 STANFORD LAW REVIEW ONLINE 88, (Feb. 13, 2012,) https://review.law.stanford.edu/wp-content/uploads/sites/3/2012/02/64-SLRO-88.pdf (last visited on 22/08/2021, 2:00 pm)
- *Kashmir Hill, (July 6, 2011).* "Revenge Porn With A Facebook Twist". *Forbes.* (last visited on 22/08/2021, 10:30 am) https://www.forbes.com/sites/kashmirhill/2011/07/06/revenge-porn-with-a-facebook-twist/?sh=4393773b1d2e
- Micheal Morris and Emily Cravigan, *The Privacy, Data Protection and Cyber Security Law Review- Australia,* (last visited on 23/08/2021)

https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/australia

- Nitesh Patel and Aayush Jain, *Government to Enhance Data Privacy and to 'Regulate the Digital Age'*, ((last visited on 23/08/2021) https://www.gclegal.com.au/limelight-newsletters/government-to-enhance-data-privacy-and-protection-to-regulate-the-digital age/?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration
- One Trust Data Guidance, Comparing Privacy Laws: GDPR v. Australian Privacy Act, https://www.dataguidance.com/sites/default/files/gdpr_v_australia.pdf (last visited on 22/08/2021 11:00 am)
- Privacy Act 1988, https://www.legislation.gov.au/Details/C2014C00076 (last visited on 22/08/2021 10:00 am)
- Renjith Mathew, *Personal Data Protection Bill, 2019 –Examined through the Prism of Fundamental Right to Privacy – A Critical Study*, (22 May 2020,) https://www.scconline.com/blog/post/2020/05/22/personal-data-protection-bill-2019-examined-through-the-prism-of-fundamental-right-to-privacy-a-critical-study/#_ftn26
- Robert Hasty Et.al, *Data Protection Law In USA*, Advocates for International Development, https://www.neighborhoodindicators.org/sites/default/files/course-materials/A4ID_DataProtectionLaw%20.pdf (visited on 22/08/2021)
- Sara Salinas and Sam Meredith, Tim Cook: Personal data collection is being 'weaponized against us with military efficiency'https://www.cnbc.com/2018/10/24/apples-tim-cook-warns-silicon-valley-it-would-be-destructive-to-block-strong-privacy-laws.html, (last visited on 25/08/2021, 09:30 am)
- Sec'y Advisory Comm. On Automated Personal Data Sys., U.S. Dept. of Health, Educ.&Welfare, Records, Computers, and the Rights of Citizens (1973) https://aspe.hhs.gov/report/records-computers-and-rights-citizens. (visited on 21/08/2021)

- Stephane Nappo, March 25, 2018, https://www.linkedin.com/pulse/digital-freedom-stops-where-users-begins-st%C3%A9phane-nappo (visited on 20/08/2021)
- Telegraphindia.com. *New data bill gives sweeping powers to govt*. https://www.telegraphindia.com/opinion/new-data-bill-gives-sweeping-powers-to-govt/cid/1726583 (Accessed 20 September 2021)

Reports

- A free and fair digital economy, protecting privacy, empowering Indians, Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, Pg-114, https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf (last visited 27/08/2021, 7:00 am)
- Report of the Group of Experts on Privacy Constituted by Planning Commission of India under the Chairmanship of Justice A.P Shah, Former Chief Justice, Delhi High Court, https://cis-india.org/internet-governance/blog/report-of-group-of-experts-on-privacy.pdf, (last visited on 25/08/2021, 10:30 am)

APPENDIX

The National University of Advanced Legal Studies, Kochi

Kalamassery, Kochi – 683 503, Kerala, India

CERTIFICATE ON PLAGIARISM CHECK

1.	Name of the Candidate	Ann Maria Sebastian
2.	Title of Thesis/Dissertation	Privacy and Data Protection in Cyberspace- A Critical Analysis of Data Protection Laws in India
3.	Name of the Supervisor	Dr. Sandeep M.N.
4.	Similar Content (%) Identified	
5.	Acceptable Maximum Limit (%)	
6.	Software Used	
7.	Date of Verification	

**Report on plagiarism check, specifying included/excluded items with % of similarity to be attached in the Appendix*

Checked By (Name, Designation &Signature) :

Dr. Sandeep M.N
Assistant Professor (Law)
NUALS, Kochi

Name and Signature of the Candidate :

Ann Maria Sebastian

Name & Signature of the Supervisor :

Dr. Sandeep M.N