# PRIVACY AS A HUMAN RIGHT IN THE DIGITAL AGE: A SOCIO-LEGAL STUDY OF SOCIAL MEDIA USERS WITH SPECIAL REFERENCE TO STUDENTS OF CENTRAL UNIVERSITIES IN UTTAR PRADESH

**THESIS**

SUBMITTED TO THE
BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY
LUCKNOW

BABASAHEB
BHIMRAO
AMBEDKAR
UNIVERSITY
LUCKNOW
प्रज्ञा शील करूणा
ESTABLISHED 1996

FOR AWARD OF THE DEGREE OF

**Doctor of Philosophy**


SUBMITTED BY
**SHIV KUMAR**
ENROLLMENT NO.- 057/16

SUPERVISOR
**Prof. (Dr.) Preeti Misra**
DEAN (SLS) & HOD(DHR)

CO-SUPERVISOR
**Dr. Rashida Ather**
ASSISTANT PROFESSOR

DEPARTMENT OF HUMAN RIGHTS
SCHOOL OF LEGAL STUDIES
BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY
(A CENTRAL UNIVERSITY)
VIDYA VIHAR, RAEBARELI ROAD
LUCKNOW-226025


2022

**DEDICATED TO**

**MY REVERED TEACHER**

**(Late) SATYENDRA NATH TANDON**

# DECLARATION

I, **Shiv Kumar**, declare that the thesis titled **"PRIVACY AS A HUMAN RIGHT IN THE DIGITAL AGE: A SOCIO-LEGAL STUDY OF SOCIAL MEDIA USERS WITH SPECIAL REFERENCE TO STUDENTS OF CENTRAL UNIVERSITIES IN UTTAR PRADESH"** has been prepared by me under the co-supervision **Dr. Rashida Ather,** Assistant Professor, Department of Human Rights, School of Legal Studies, Babasaheb Bhimrao Ambedkar University (A Central University) Lucknow and supervision of **Prof. (Dr.) Preeti Misra,** Head - Department of Human Rights, Dean - School of Legal Studies, Babasaheb Bhimrao Ambedkar University (A Central University) Lucknow, 226025. No part of this thesis has formed the basis for the award of any degree, diploma or fellowship previously.

Further, I declare that the material embodied in the present work is based on original research work and the indebtedness to others has been duly acknowledged at relevant places. I also declare that the thesis is essentially free from all kinds of plagiarism.

Date: 13.07.2022

**Shiv Kumar**
Research Scholar,
Department of Human Rights,
School of Legal Studies,
Babasaheb Bhimrao Ambedkar University
(A Central University),
Vidya Vihar, Raebareli Road,
Lucknow-226025 (U.P)

बाबासाहेब भीमराव अम्बेडकर विश्वविद्यालय
(केन्द्रीय विश्वविद्यालय)
विद्या विहार, रायबरेली रोड, लखनऊ–226025
BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY
(A Central University)
Vidya Vihar, Raebareli Road, Lucknow-226025
Accredited 'A' Grade by NAAC in 2015

Letter No:.....

Date:.....

# CERTIFICATE

This is to certify that the thesis titled **"PRIVACY AS A HUMAN RIGHT IN THE DIGITAL AGE: A SOCIO-LEGAL STUDY OF SOCIAL MEDIA USERS WITH SPECIAL REFERENCE TO STUDENTS OF CENTRAL UNIVERSITIES IN UTTAR PRADESH"** submitted by **Mr. Shiv Kumar** is an original research work and has not been previously submitted in part or full for the award of any other degree or diploma to this or any other university.

The thesis submitted to Babasaheb Bhimrao Ambedkar University, Lucknow satisfies all the requirements as stipulated in the Doctor of Philosophy (Ph.D.) regulations, 2016 as amended in 2017 and it is fit for submission and evaluation for the award of the degree of Doctor of Philosophy of the University.

Co-Supervisor

(Dr. Rashida Ather)

13/07/2022

Supervisor

Prof. (Dr.) Preeti Misra

Head of the Department,
Department of Human Rights

Date:

# ACKNOWLEDGEMENT

*I express my deep sense of gratitude towards **the Samma-Sambuddha**, the Enlightened One, and **Babasaheb Dr. Bhimrao Ambedkar**, a symbol of knowledge, and architect of the Indian Constitution, who presented himself as a role model for others by acquiring the highest degrees in the void of needed resources, has always been a source of inspiration for me.*

*I am sincerely thankful to my revered supervisor **Prof. Preeti Misra,** Head, Department of Human Rights and Dean, School of Legal Studies, for her able supervision, persistent guidance, and continuous encouragement in the completion of my thesis. I am also thankful for her patience, motivation, and immense knowledge.*

*Besides my supervisor, I would like to express my deep sense of gratitude to **Prof. Priti Saxena,** Director, CPGLS, School of Legal Studies, BBAU Lucknow, for her mental support and valuable guidance whenever I needed it.*

*I am also thankful to my co-supervisor, **Dr. Rashida Ather,** Department of Human Rights, School of Legal Studies, Babasaheb Bhimrao Ambedkar University, Lucknow, for her insightful comments, determined encouragement, and wise counseling in my crucial time. My sincere thanks also go to **Dr. Rashwet Shrankhal, Dr. Ajay Kumar Kushwah,** and **Dr. Vijay Bhaskar,** Department of Human Rights, School of Legal Study, Babasaheb Bhimrao Ambedkar University, Lucknow.*

*I express my deep gratitude towards **Rev. S. N. Goenka Ji** (Principal Teacher of Vipassana, Padmavibhushan Awardee by the Government of India) and **Rev. S. N. Tandon Ji** (A Great Scholar, philanthropist, and prominent administrator), **Dr. Omdutt Triapthi Ji, Ms. Rashmi Sobti ji** for their blessings, inspiration, moral support to accomplish the present work. In the void of their blessings, inspiration, and moral support the present work would not have been possible.*

*I am also grateful to the library staff of Ram Manohar Lohia National Law University, Lucknow, and Gautam Buddha Central Library, Babasaheb Bhimrao Ambedkar University, especially **Dr. O. P. Saini**, assistant librarian GBL, BBAU for sparing his valuable time from his hectic schedule in providing me with his valuable guidance, moral support wherever I needed.*

*I am also very thankful to* ***Dr. Pravish Prakash,*** *Deputy Librarian, Tagore Library, Lucknow University for his valuable guidance and for providing different resources from time to time. I also extend my thanks to* ***Dr. Priyanka Bhadouriya,*** *District Economics & Statistical Officer, Lucknow for her guidance and support at every stage of my work.*

*I am also very thankful to my seniors respected* ***Dr. Pramod Kumar, Dr. Satyendra Kumar Maurya, Dr. Maninder Kumar Singh, and Dr. Manjari Rawal*** *for extending their helping hands whenever I needed them.*

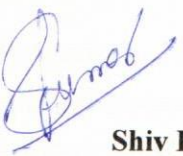
*I would like to record my thanks to all my fellow research scholars especially* ***Mr. Jitendra Kumar Saroj, Mr. Prashant Tripathi, Ms. Deepika Rani,*** *and* ***Ms. Shivpriya****, Department of Human rights as well as* ***Dr. Shalini Singh Tomar, Mr. Sateesh Kumar,*** *and* ***Mr. Irshad Ahmad*** *Department of Law, School of Legal Studies, BBAU Lucknow for their valuable suggestions, stimulating discussions, and cooperation regarding my research work.*

*I record my sincere thanks to the people who helped me during data compilation and review of the document* ***Mr. Mukesh Kumar Bharti*** *(Research Scholar, Lucknow University),* ***Mr. Avinash Sandilya*** *(Research Scholar, University of Allahabad),* ***Mr. Deepak Yadav*** *(Research Scholar, DHR, BBAU),* ***Mr. Yogesh Verma, Mr. Abhishek Kumar, Mr. Firoj Babu*** *(Students of BBAU).*

*I put my special thanks and indebted to all authors, and writers whose work has been utilized by me in this present research study.*

*This journey of my academic path could not have been possible without the loving-kindness and compassion of members of my Dhamma family, especially* ***Mr. Gopal Sharan Singh, Ms. Pushpa Singh, Dr. Anil Kumar Maurya, Mr. Naresh Kumar, Ms. Rekha, Mr. Rajendra Kumar, Mr. Rajesh Malik, Mr. Jalaj Ruhela*** *and* ***Mr. Abhay Kumar****.*

*This study could not have been possible without the moral support of my family. My parents and other members -* ***Mr. Siyaram*** *(Uncle),* ***Ms. Lalita Devi*** *(Sister) were constant source of encouragement for me.*



**Shiv Kumar**

# PREFACE

Privacy is an issue of profound importance around the world. Social media and social networking sites (SNS) have risen sharply in popularity and widespread use, allowing new forms of socialization, sharing, and communication between people. This new state of communication raises new privacy questions.

Online self-disclosure of personal information by social media users lies at the heart of the problem posed by social media. We are now beginning to realise that, on occasion, social media and other websites can have a dark side.

The researcher has analysed various privacy issues connected with social media. Privacy policies of social media are difficult to understand and contain ambiguous language. Privacy policies tend to be long boring documents with ambiguous and misleading language. Most of the users do not read them. Although young people claim, or appear to be, both concerned about and aware of privacy issues, they usually do not take any precautionary measures to protect themselves.

Social media that are based on targeted advertising continuously monitor and record personal data and online activities of the users. They store, merge and analyse collected data. This allows them to create detailed user profiles and to know a lot about the users' personal interests and online behaviours. This personal data of users is sold by social media to other advertising clients.

The report on **'**The Right to Privacy in the Digital Age 2014," recommended that States should review their own national laws, policies and practices to ensure full conformity with international human rights law. A clear, precise, accessible, comprehensive, and non-discriminatory legislative framework is required in every State. An effective remedy should be provided to the victims.

Although there are wide and continuous recommendations of the United Nations to protect "the right to privacy in the digital age" by the states as well as business enterprises but there is a huge implementation gap at the national level and among the business enterprises.

India does not have any specific data protection mechanism. Statutory protection of privacy can be found in India is scattered across a number of statutes.

Despite all international obligations of India, recommendations given by the United Nations as well as Puttaswamy Constitutional Bench decision to enact data protection law, the Government of India has still a lot of work to be done to achieve the aspirations of these organizations.

In this study, the researcher has tried to discuss how privacy is being transformed to new forms and new concepts like privacy by design, intellectual privacy, etc. are evolving in the digital age. Privacy is associated with surveillance and data protection. This discussion will really enhance the existing knowledge on the issue of privacy in the digital age.

The researcher has examined the role of national as well as international laws in the protection of privacy of individuals on social media platforms. Adherence to the data protection principles by the social media while processing information of users, rights of data subjects, privacy by design during the development process, due diligence, and triple test (legality, necessity, and proportionality) are some legal issues discussed by the researcher. It is hoped that this research will help the state as well as business enterprises to fulfill the legal and moral commitment in order to protect, and respect the right to privacy of individuals and provide a remedy in case of violation of privacy.

Through the survey of students of central universities in Uttar Pradesh, the researcher has tried to know the awareness level regarding legal provisions and privacy policies of social media. The findings will really help the social media users and authorities to know the value of personal information in the digital age, shared with social media, and develop a mechanism to protect and respect the right to privacy of the individuals. Hence, the suggestions and recommendations will strengthen the human rights approach to the right to privacy in the digital age.

# CONTENTS

# CHAPTER III

# PRIVACY POLICIES OF SOCIAL MEDIA

## CHAPTER IV

## PRIVACY LAWS & SOCIAL MEDIA: INTERNATIONAL PERSPECTIVE

## CHAPTER V

## PRIVACY LAWS & SOCIAL MEDIA: INDIAN PERSPECTIVE

CHAPTER VI

DATA ANALYSIS AND INTERPRETATION

## CHAPTER VII



## APPENDICES

# LIST OF ABBREVIATIONS

| | |
|---|---|
| **AI** | **Artificial Intelligence** |
| **AMU** | **Aligarh Muslim University** |
| **APEC** | **Asia Pacific Economic Corporation** |
| **BBAU** | **Babasaheb Bhimrao Ambedkar University** |
| **BHU** | **Banaras Hindu University** |
| **CJEU** | **Court of Justice of the European Union** |
| **CoE** | **Council of Europe** |
| **COVID** | **Coronavirus disease** |
| **CSR** | **Corporate Social Responsibility** |
| **DARE** | **Department of Agricultural Research and Education** |
| **DPA** | **Data Protection Act** |
| **DPbD** | **Data Protection by Design** |
| **DPD** | **Data Protection Directive** |
| **EC** | **European Council** |
| **ECHR** | **European Convention on Human Rights** |
| **ECtHR** | **European Court of Human Rights** |
| **EU** | **European Union** |
| **GAIL** | **Gas Authority of India** |
| **ICT** | **Information and Communication Technology** |
| **IT** | **Information Technology** |
| **IIT** | **Indian Institute of Technology** |

| | |
|---|---|
| **UNHRC** | **UN Human Rights Committee** |
| **HRL** | **Human Rights Law** |
| **ICCPR** | **International Covenant on Civil and Political Rights** |
| **IHL** | **International Humanitarian Law** |
| **IPC** | **Indian Penal Code** |
| **NHRC** | **National Human Rights Commission** |
| **NSA** | **The National Security Act,** |
| **OHCHR** | **Office of the High Commissioner for Human Rights** |
| **OIDB** | **Oil Industry Development Board** |
| **ONGC** | **Oil and Natural Gas Commission** |
| **PbD** | **Privacy by Design** |
| **PPP** | **Public-Private Partnership** |
| **RtbF** | **Right to Be Forgotten** |
| **SNS** | **Social Networking Sites** |
| **UDHR** | **Universal Declaration of Human Rights** |
| **UK** | **United Kingdom** |
| **UN** | **United Nations** |
| **UNDP** | **United Nations Development Programme** |
| **UNGA** | **United Nations General Assembly** |
| **UNGP** | **United Nation Guiding Principles** |
| **UNOHCHR** | **United Nations Office of the High Commissioner for Human Rights** |
| **UNSC** | **United Nations Security Council** |

# LIST OF CASES

# LIST OF TABLES AND FIGURES

**Tables:**

**Figures:**

# CHAPTER-I

# INTRODUCTION

# CHAPTER I
# INTRODUCTION

## 1.1 INTRODUCTION

The first two decades of the twenty-first century have seen a simultaneous proliferation of new technological threats to and opportunities for international human rights. New advances in area of – not only the Internet, social media, and artificial intelligence but also the novel techniques for controlling reproduction or dealing with climate change – make clear that scientific and technological innovations bring both risks and benefits to human rights.[1]

Data has become an indispensable component of the internet and therefore, the economy. Some of the largest companies in the world have built business empires around the collection and processing of data. This massive pool of data collected by these companies allows them to invade the private lives of an individual, and in more cases than not, without the individual's consent. These companies have been able to escape from the consequences of these intrusions because of a principle that lies at the very foundation of the internet i.e., self-regulation.[2]

### 1.1.1 PRIVACY

Privacy is an issue of profound importance around the world. Privacy as a basic human right touches upon fundamental needs and values associated with man's gregarious nature.

Privacy enjoys an abundance of meanings. It is claimed in diverse situations every day by everyone against other people, society, and the state.[3]

Privacy is a sweeping concept, encompassing *inter alia* freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations.[4]

---

[1] Molly K. Land and Jay D. Aronson (eds.), *New Technologies for Human Rights Law and Practice,* 1 (Cambridge University Press, New Delhi, 2018).
[2] Vishal Rakhecha and Chittkrishna Thakkar, *Data Localisation And Enforcement Of The Right To Privacy,* 5 CMET (2018) 102, *available at:* SCC Online Web Edition: http://www.scconline.com (last visited on May 30, 2022).
[3] Bhairav Acharya, "The Four Parts of Privacy in India" 50 (22) *Economic and Political Weekly* 32 (May 30, 2015).
[4] Daniel J. Solove, *Understanding Privacy* 1 (Harvard University Press, USA, 2008).

Privacy as a concept is elusive. It's not because it is hard to define, but because it's pretty dynamic, influenced by individual choices of privacy and their rights as defined worldwide by various regulatory authorities or governments and changes in the political and technological environment.[5]

Today, in the backdrop of the ubiquitous presence of the internet, the right to privacy has come to be understood as a multifaceted right meaning thereby that privacy is no more concerned with the physical aspect only, it includes within its ambit the communication privacy and information privacy as well. This digital age has given a multidimensional sphere to the concept of privacy protection.[6]

Privacy is at least in some ways about control over how much is known about us by whom. In the online world, where decisions are made on the basis of information – or data – that aspect of privacy becomes particularly significant. To protect our autonomy, to have influence over what happens to us online, over what we see online, over what decisions are made about us and for us, we need to have protection over how data is gathered about us, how that data is used, who can hold that data and so forth.[7]

The right to privacy safeguards an individual's dignity by protecting their personal information from public scrutiny.[8]

Privacy is linked to both positive and negative freedoms. In terms of positive freedom, privacy expresses the set of rights for a person's ability to control four broad areas of legal concern: freedom of personal autonomy; the right to control personal information; the right to control property; and the right to control and protect physical space. As a negative freedom, privacy is understood as the absence of invasion of privacy by the government, business, or other actors into the space considered personal.[9]

---

[5]Gunasundaram, *Importance Of Data Privacy In The Digital Era, available at:* https://medium.com/gunasundaram/importance-of-data-privacy-in-the-digital-era-fd323bb4a40d (last visited on May 30, 2022).

[6] Human right and Social media *available at* "https://www.researchgate.net/publication/331715928_Human_Right_and_Social_Media (last visited on 22.01.2020)

[7] Bernal, Paul, *Internet Privacy Rights* 15 (Cambridge University Press, United Kingdom, 2014).

[8] Privacy In The Digital Age | Why Digital Privacy Is Important, *available at:* https://www.filecloud.com/blog/2019/02/data-privacy-in-a-digital-age/#.YqlYCKFBxPY (last visited on May 30, 2022).

[9]Monroe E. Price, Stefaan G. Verhulst and Libby Morgan et.al. (eds.), *Routledge Handbook of Media Law* 470 (Routledge, New York, 2013).

### 1.1.2 PRIVACY AS A HUMAN RIGHT

Human rights are universal. All human beings are legally eligible to enjoy human rights for one simple reason – they are human. Human rights are codified in a body of international law. To protect human rights, there exist international human rights instruments. These international instruments consist of treaties and other international documents, basically classified as Declarations and Conventions. The UN General Assembly adopted the Universal Declaration of Human Rights (hereinafter, "UDHR") in 1948, but this declaration does not have binding force. Nevertheless, UDHR as a Bible on human rights is *jus cogens*. On the other hand, conventions are binding under international law. The United Nations has set out a broad spectrum of rights by drafting the most important human rights regime known as the "International Bill of Rights". Each of the documents proclaims a list of basic human rights: The Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), and the International Covenant on Economic, Social, and Cultural Rights (ICESCR). The human rights set out in these instruments are supplemented by a range of other international treaties – however, these treaties rarely refer expressly to the protection of human rights through technology (Australian Human Rights Commission 2018). Besides the international regime of human rights law, there are regional and domestic institutions and organizations; these regional and domestic institutions and organizations provide well-developed remedial frameworks - the application of human rights law to changing circumstances (including technological developments) is also well articulated.[10]

The right to privacy as a human right is firmly established in international law conventions. Therefore, the position of privacy in the catena of human rights is universally accepted.

Article 12[11] of the Universal Declaration of Human Rights (1948) and Article 17[12] of the International Covenant on Civil and Political Rights protect individuals'

[10] Prof. Priti Saxena, "Technological Advancements: Enriching or Violating Human Rights?" 20 *Journal of The National Human Rights Commission, India* 33-34 (December 10, 2021).

[11] The Universal Declaration of Human Rights, 1948, art. 12.
It states as follows:
"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."

[12] The International Covenant on Civil and Political Rights, 1966, art. 17.
It states as follows:
"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."

privacy, honour and reputation, their families, home, and correspondence against any arbitrary interference.

In order to be consistent with international human rights law, an interference with a qualified right such as privacy must meet the tests of legality, necessity, and proportionality. In terms of legality, the action constituting the interference (such as interception of communications) must be previously established in a law that is publicly accessible, clear, and precise, meaning that its consequences are foreseeable. Interference must be in pursuit of a legitimate aim, and it must be a necessary and proportionate means of achieving that aim. For the European Court of Human Rights, the measure must be "necessary in a democratic society," meaning that it must answer a "pressing social need," and state authorities must provide "relevant and sufficient" justifications for the measure.[13]

The report on 'The Right to Privacy in the Digital Age 2014," recommended that States should review their own national laws, policies, and practices to ensure full conformity with international human rights law. A clear, precise, accessible, comprehensive, and non-discriminatory legislative framework is required in every State. An effective remedy should be provided to the victims.[14]

### 1.1.3 PRIVACY AND SOCIAL MEDIA

Concern with the right of privacy increased in the 1960s and 1970s with the advent of information technology (IT).[15] One of the great innovations of the 1990s and beyond is the sudden and rapid growth of social media, or social networking sites, which permit people to communicate quickly and easily through the Internet.[16]

Privacy is rapidly becoming inextricably linked to the world of digital communications and social media. Social media and social networking sites (SNS) have risen sharply in popularity and widespread use, allowing new forms of socialization, sharing and communication between people. This new state of communication raises new privacy questions.

---

[13] *Supra* note 1 at 225-226.
[14] UN General Assembly*, The right to privacy in the digital age,* GA Res 27/37, GAOR, UN Doc A/HRC/27/37 (June 30, 2014). *available at*: http://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc (last visited on May 30, 2022).
[15] S. R. Chauhan and N.S. Chauhan (eds.), *International Dimensions of the Human Rights,* Vol. 2, 691 (Global Vision Publishing House, New Delhi, 2006).
[16] Stephen Currie, *How is the Internet eroding the privacy rights* 25 (Reference Point Press, 2014).

Digital platform, termed 'social media', is the main form of communication, based on networking broadcast, telecast information through social networking sites Facebook, WhatsApp, Twitter, Orkut, My space, Instagram, etc. Social media has a profound impact on the right to privacy and freedom of speech and expression.[17]

Social Networking Sites like Facebook, Google and many others are violating the privacy of users through economic surveillance. Economic surveillance on corporate social media is surveillance of prosumers, who keeps on creating and sharing user-generated content, browse profiles and data, interact with others, join, create and build communities and co-create information. The corporate web platform operators and their third-party advertising clients continuously monitor and record personal data and online activities. They store, merge and analyse collected data. This allows them to create detailed user profiles and to know a lot about the users' personal interests and online behaviours. Social media that are based on targeted advertising sell prosumers as a commodity to advertising clients. There is an exchange of money for access to user data that allows economic user surveillance.[18]

In K. S. Puttiswamy v Union of India[19], Supreme Court held that "Right to privacy is an intrinsic part of the right to life and personal liberty." This right has become more vulnerable in times of social media. Broadly, privacy can be explained under two broad categories- privacy against the State and privacy against non-state actors. The former includes personal data and records of information in the public domain which are kept in the hands of State authority; the State is under obligation to respect the privacy of the said individual and not disclose or disseminate their data freely, and the second includes the non-state actors like Uber, Ola, social networking, and payments websites where the records of conversations- both personal and professional, movements & locations, shopping habits, health, etc. - are with the privacy authority. Many times, these websites are hacking in cyberspace which sacrificed personal information of citizens.

Every social media website has a privacy policy. The purpose of a privacy policy is to outline how organizations will collect, maintain, and share user data. Often

[17] *Supra* note 10 at 47.
[18] Christian Fuchs, *Social Media: A Critical Introduction,* 108 (Sage Publications, New Delhi, 2014).
[19] (2017) 10 SCC 1.

organizations write the privacy policy in a way that protects the organization more than the user.[20]

The report[21] of the United Nations High Commissioner for Human Rights, mandated by the Human Rights Council in its resolution 42/15 highlighted that the widespread use of artificial intelligence, including profiling, automated decision-making, and machine-learning technologies, by States and businesses affects the enjoyment of the right to privacy and associated rights.

## 1.2 STATEMENT OF PROBLEM

The United Nations General Assembly in 2013 adopted Resolution 68/167 relating to the right to privacy in the digital age wherein it has clearly acknowledged the concern over increasing issues of eroding privacy protection in this technologically advanced world. The relevant portion of the preamble reads as

*"Noting that the rapid pace of technological development enables individuals all over the world to use new information and communication technologies and at the same time enhances the capacity of governments, companies, and individuals to undertake surveillance, interception and data collection, which may violate or abuse human rights, in particular the right to privacy, as set out in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights, and is, therefore, an issue of increasing concern.[22]*

Considering the potential threats in the form of communication surveillance, its interception, data theft, unauthorized personal data access, trans-border flow of data etc. the UN has affirmed that the same rights that people have offline must also be protected online, including the right to privacy.[23]

In the wake of COVID-19, the use of information and communication technology and surveillance by the State has met at cross-roads and has given much leeway for the

[20]A. W. Haynes, "Online privacy policies: Contracting away control over personal information" *Penn State Law Review* 111, 587 (2007).
[21] UN General Assembly, Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General *The right to privacy in the digital age,* UN Doc A/HRC/48/31 (September 13, 2021). a*vailable at:* https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/249/21/PDF/G2124921.pdf?OpenElement (last visited on May 30, 2022).
[22] Dr. Lisa P Lukose ET. AL., Human right and Social media. available at https://www.researchgate.net/publication/331715928_Human_Right_and_Social_Media (last visited on Feb 22, 2022).
[23] The right to privacy in the digital age : report of the Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age : (un.org) (last visited on Feb. 22, 2022).

State to cause mass surveillance. In the name of locating, contacting, screening, flagging, monitoring, and isolating those affected by the virus. The application is used for mass surveillance and also for accessing user information. Also, it cannot be denied that totalitarian regimes would use absolute access to restrict the individuals' civil liberties arbitrarily. Excessive monitoring creates a surveillance State, where everyone's body, mind and soul are under continuous supervision.[24]

In Puttaswamy[25] Case it was held that "Informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the state but from non-state actors as well". The Court further observes the following to explain the nature and unlimited extent of invasion of privacy through internet usage:

"*Popular websites install cookie files by the user's browser. Cookies can tag browsers for unique identified numbers, which allow them to recognise rapid users and secure information about online behaviour. Information, especially the browsing history of a user is utilised to create user profiles. The use of algorithms allows the creation of profiles about internet users. Automated content analysis of e-mails allows for reading of user e-mails. An e-mail can be analysed to deduce user interests and to target suitable advertisements to a user on the site of the window. The books which an individual purchases online provide footprints for targeted advertising of the same genre. Whether an airline ticket has been purchased in economy or business class, provides vital information about employment profile or spending capacity. Taxi rides booked online to shopping malls provide a profile of customer preferences. A woman who purchases pregnancy-related medicines online would be in line to receive advertisements for baby products. Lives are open to electronic scrutiny. To put it mildly, privacy concerns are seriously an issue in the age of information."*

The popularity of social networking sites such as Facebook, Twitter, and Instagram to name a few is not hidden from anybody. The craze with which people specially the younger generation are found glued to these social networking sites one would not be wrong to term the craze as addiction.

Young people are said to be less concerned with their privacy and to value their privacy less compared to older people. This view rests mainly on studies that show that

[24] Yuthika Bhargava, "Hacker sees security flaws in Arogya Setu" *Th Hindu,* May 06, 2020.
[25] *Supra note* 19.

young people share a great deal of information on social network sites and anecdotal reports in the media, which show how such disclosures can lead to personal misfortune.[26]

Social media is a fast-growing phenomenon in India, as more and more young Indians are getting access to smartphones and the internet. With 250+ million social network users, India has the second-highest number of social media users in the world. Facebook, YouTube, and WhatsApp dominate the social media space in India. While Instagram is also very popular amongst urban Indian youth.[27]

About two-thirds of Indian youth perceive addiction to social media, loss of privacy, fake news, and cyberbullying as potential risks of social media.[28]

In recent years there has been an increasing awareness that a high level of data protection is essential to foster people's trust in online services and in the digital economy in general. Privacy concerns are among the top reasons for people not buying goods and services online. With the technology sector directly contributing to 20% of overall productivity growth in Europe and 4% of overall investment aimed at the sector, individual trust in online services is vital for stimulating economic growth in the EU.[29]

In today's global economy, the importance of strong, enforceable, and internationally interoperable data protection standards cannot be underestimated. This is very true for India, as it has sought, and is seeking to position itself as an attractive destination for business and data processing. To help achieve this goal, India sought 'data secure' status from the European Union in 2012 as part of negotiations on the free trade agreement with the region. According to the Data Security Council of India, if India were to receive adequacy, the Indian out-sourcing sector could increase from $20 billion to $50 billion annually. For many years, India has also been seeking membership to the Asia-Pacific Economic Cooperation (APEC).[30]

---

[26] Wouter M. P. Steijn and Anton Vedder "Privacy under Construction: A Developmental Perspective on Privacy Perception" 40 (4) *Science, Technology, & Human Values* 616 (July 2015).
Stable URL: https://www.jstor.org/stable/43671276

[27] Social Media for Youth and Civic Engagement in India, page 11 (2019) *available at*: https://www.coursehero.com/file/80975786/SOCIAL-MEDIA-REPORTpdf/ (last visited on May 30, 2022).

[28] *Ibid.*

[29] The European Commission issued a consultation paper titled '*Safeguarding Privacy in a Connected World'* (January 25, 2012). *available at:*
http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_9_en.pdf (last visited on May 30, 2022).

[30] David J. Kessler, Sue Ross and Elonnai Hickok, "A Comparative Analysis of Indian Privacy Law and The Asia-Pacific Economic Cooperation Cross-Border Privacy Rules" 26 (1) *National Law School of India Review* 31-32 (2014).

## 1.3. REVIEW OF LITERATURE

The researcher has presented briefly herein the information collected from comprehensive literature. Many books, articles, and reports have been reviewed by the researcher. Some of these are as follows:

**A User's Guide to Data Protection,** Bloomsbury (2016), this book is a clear and accessible guide to the data compliance issues that organisations must adhere to. It provides assistance with understanding UK data protection rules and regulations, along with a full assessment of the new EU rules and their impact on practice.

**Cyber Law,** Pawan Duggal (2022), the author has presented an exhaustive section-wise commentary on the Information Technology Act along with Rules, Regulations, Policies, and Notifications etc. As the author has emphasized that Cyberlaw 3.0 is also likely to deal with new challenges faced by SOLOMO (Social-Location-Mobility) which is a combination of social media, use of mobile devices, and information about location of individuals. This book has helped the researcher to have better insight into privacy from the technological point of view.

**Data Privacy Law *An International Perspective,*** Lee A. Bygrave (2014), the researcher found this book highly informative for the purpose of acquiring an understanding of the core principles and mechanics of data privacy law. This book goes where others have feared to tread. It goes beyond a simple analysis of national legislation into a global survey of the provisions and directions of the burgeoning law on this topic.

**Emerging Challenges in Privacy Law,** edited by Normann Witzleb, David Lindsay, Moira Paterson, Sharon Rodrick (2014), this collection of essays explores current developments in privacy law, including reform of data protection laws, privacy and the media, social control, and surveillance, privacy and the Internet, and privacy and the courts. It places these developments into a broader international context, with a particular focus on the European Union, the United Kingdom, Australia, and New Zealand. Adopting a comparative approach, creates an important resource for understanding international trends in the reform of privacy and data protection laws across a variety of contexts.

**Handbook of Social Media and the Law,** Laura Scaife (2015), this book considers the significant legal developments that have arisen due to social media. It provides an expert explanation of the issues those practitioners and business need to

consider, as well as the special measures that are required in order to minimise their exposure to risk. Various categories and channels of social media are covered in this book, alongside the legal classification of different social networks.

**Information Politics, Protests, and Human Rights in the Digital Age,** edited by Mahmood Monshipouri (2016), we live in a highly complex and evolving world that requires a fuller and deeper understanding of how modern technological tools, ideas, practices, and institutions interact and how different societies adjust themselves to the emerging realities of the digital age. This book conveys such issues with a fresh perspective and in a systematic and coherent way. This edited collection provides a balanced conceptual framework to demonstrate the power of autonomous communication networks and their limits and the increasing setbacks they encounter in different contexts.

**Information Technology Law and Practice,** Vakul Sharma & Seema Sharma (2021), authors have presented section-wise commentary capturing the journey of the Information Technology Law with important case laws including landmark judgment of Aarogya Setu, privacy, Freedom of Speech and Expression, criminal defamation and child pornography. This book helped the researcher to scrutinise the role of intermediaries, streaming services/Over-the-top media platforms, Apps, Privacy protocol, and blocking for public access.

**Intellectual Privacy Rethinking Civil Liberties in the Digital Age,** Neil Richards (2015), the author shows how privacy and free speech are often essential to each other. He explains the importance of "intellectual privacy". By this, he means protection from surveillance or interference when we are engaged in the processes of generating ideas – thinking, reading and speaking with confidantes before our ideas are ready for public consumption. In our digital age, in which we increasingly think, read, and communicate with the help of technologies that track us, increased protection for intellectual privacy has become essential.

**Internet Privacy Rights - Rights to Protect Autonomy,** Bernal Paul (2014), this book focuses on Internet Privacy Rights analysis of the current threats to our online autonomy and privacy and proposes a new model for gathering, retention and use of personal data. Key to the model is the development of specific privacy rights: a right to roam the internet with privacy, a right to monitor the monitors, a right to delete personal data, and a right to create, assert and protect online identity. These rights could help in

the formulation of more effective and appropriate legislation, and shape more privacy-friendly business models.

**Legal Research Methodology,** Dr. S. R. Myneni (2013), although there is number of books on research methodology for Social Sciences. But, this book focussed on legal aspects of research methodology has really proved beneficial for the researcher.

**New Technologies for Human Rights Law and Practice,** edited by Molly K. Land & Jay D. Aronson (2018), this book focuses on how technology affects the enjoyment of human rights. Cross-cutting themes – power and justice, accountability, and the role of private authority have been identified and analysed to chart a road map for further study of the relationship between technology and human rights. This book addresses how human rights law can and should respond to the growth in private authority that results from the introduction of new technologies.

**Research Design, Qualitative, Quantitative, and Mixed Method of Approaches,** John W. Creswell (2014), this book advances a framework, a process, and compositional approaches for designing a proposal for qualitative, quantitative, and mixed methods research in the human and social sciences. The ascendency of qualitative research, the emergence of mixed methods approaches, and the continuing use of the traditional forms of quantitative designs have created a need for this book's unique comparison of the three approaches to inquiry. This comparison begins with a preliminary consideration of philosophical assumptions for all three approaches, a review of the literature, an assessment of the use of theory in research approaches, and reflections on the importance of writing and ethics in scholarly inquiry. The book then addresses the key elements of the process of research: writing an introduction, stating a purpose for the study, identifying research questions and hypotheses, and advancing methods and procedures for data collection and analysis.

**Research Methodology Methods and Techniques,** C. R. Kothari (2004), this book has been very helpful to the researcher in adopting the most appropriate methodology for research study; and to make him familiar with the art of using different research methods and techniques specially in terms of drafting questionnaire, choosing appropriate sampling method.

**Routledge Handbook of Media Law,** edited by Monroe E. Price, Stefaan G. Verhulst & Libby Morgan (2013), this book provides an authoritative survey of media law from a comparative perspective. It provides a better understanding of the forces that generate media rules, norms, and standards against the background of major

transformations in the way information is mediated as a result of democratization, economic development, cultural change, globalization and technological innovation.

**Social Media a critical introduction, Christian Fuchs (2017),** this book equips with the critical approach that readers need to understand the complexities and contradictions of social media and the information society. This book provided the researcher with essential text about new media world. A definitive book for all social media users who long for dignity, freedom, and a more democratic Internet – illuminated by critical theory.

**Social Media and Democracy,** edited by Brian D. Loader & Dan Mercea (2012), this book critically investigates the complex interaction between social media and contemporary democratic politics and provides a grounded analysis of the emerging importance of social media in civic engagement.

**Social Media and the Law A Guidebook for communications Students and Professionals,** edited by Daxton R. Stewart (2017), this book examines current issues like copyright, online impersonation, anonymity, cyberbullying, sexting, live streaming, defamation, privacy, intellectual property relating to emerging law in key areas of social media. This book is to help students, researchers, and professional communicators navigate the tricky legal terrain of social media. This book has been a boon for the researcher in serving as a go-to- resource for being so thorough and comprehensive in examining nearly all the key legal issues.

**The Digital Person Technology and Privacy in the Information Age,** Daniel J. Solove (2004), this book is about how we should understand and protect privacy in light of profound technological developments. Much of the law pertaining to privacy is based on old conceptions of privacy, and as a result, it has failed to resolve the emerging privacy problems created by digital dossiers. This book aims to rethink longstanding notions of privacy to grapple with the consequences of living in an Information Age.

**Understanding Privacy,** Daniel J. Solove (2008), this book deals with the immense complexity, philosophical richness, and contemporary relevance of privacy. This book is the product of many years of conversations between the author with other scholars. Portions of this book were adapted from the articles bearing the titles: 'Conceptualizing Privacy', 'The Virtues of Knowing Less: Justifying Privacy Protections against Disclosure', and 'A Taxonomy of Privacy' published in different journals and reproduced with the author's arguments.

**Understanding Social Media,** Varinder Taprial & Priyanka Kanwar (2012), this book discovers how social media has transformed over the years, what benefits it brings to individuals and businesses and why social media management is important. The authors have also discussed some tools, which are useful to manage users' social media activities.

**Understanding Social Media,** Sam Hinton & Larissa Hjorth (2013), Understanding Social Media attempts to engage with some of the complex debates about the definitions of social media. The book reflects upon the differences between SNSs and social media and how the rise in devices such as smartphones and locative media services such as Facebook Places, Google Maps, and Foursquare are changing the fabric of social media. The authors acknowledge that social media is currently transforming definitions of both 'social' and 'media'.

**RESEARCH PAPERS/ ARTICLES IN JOURNAL**

**A Behavioural Understanding of Privacy and its Implications for Privacy Law** by Kirsty Hughes, *The Modern Law Review,* Vol. 75, No. 5 (September, 2012). The author has discussed the right to privacy based on social interaction theory. This theory states that the right to privacy is a right to respect for barriers and that an invasion of privacy occurs when a privacy barrier is penetrated.

**A Comparative Analysis Of Indian Privacy Law And The Asia-Pacific Economic Cooperation Cross-Border Privacy Rules** by David J. Kessler, Sue Ross and Elonnai Hickok, *National Law School of India Review,* Vol. 26, No. 1 (2014). Published by: Student Advocate Committee. Authors have argued that in today's global economy, and particularly for India, the importance of strong, enforceable, and internationally interoperable data protection standards cannot be underestimated. While India has adopted various sectoral laws and policies for securing data protection, most significantly the Information Technology Act and the Rules thereunder, holistic national legislation on privacy rights is absent. Such an attempt can be seen in the October 2012 Report of the Group of Experts on Privacy, which sets out nine National Privacy Principles. This paper examines the Report in the backdrop of the privacy principles of the APEC and the Information Technology Rules in light of the Cross-Border Privacy Rules. It concludes that if India is to become a member of APEC, while the principles in the Report reflect many of the principles central to the APEC privacy

framework, it must expand a few aspects of its privacy requirements under the Rules to align them more perfectly with the Cross-Border Privacy.

**Asking for Facebook Logins: An Egoist Case for Privacy** by John R. Drake, *Journal of Business Ethics*, Vol. 139, No. 3 (December 2016) Published by: Springe. The author has argued that with the advent of social networking websites, privacy concerns have reached a new height. Employers requesting login credentials to popular social media platforms of employers posed a serious threat to privacy of individuals. Many people may consider this request unethical. The author articulated how one egoist perspective provides a defence of privacy in the face of unjust information access requests. By applying Objectivist principles to a business context, we observe that businesspeople should not violate other people's privacy for short-term gains.

**Non-Informed Consent Cultures: Privacy Policies and App Contracts on Facebook** by Anja Bechmann, *Journal of Media Business Studies* (16 Mar, 2015). The author has highlighted that Social networking sites collect extensive personal and sensitive user data across a wide range of services and users accept this through a click on the accept button in their end-user license agreements (EULAs). By comparing existing regulation and discussion on future adjustments with studies of consent practices on Facebook, the article argues that with the growing importance and use of these services the consent culture of the internet has turned into a blind non-informed consent culture, heavily relying on social incentives and group dynamics in decision-making that are not adequately reflected in current and upcoming privacy regulation.

**Philosophical Theories of Privacy: Implications For an Adequate Online Privacy Policy** by Herman T. Tavani, *Metaphilosophy* Vol. 38, No. 1 (January 2007). The author has critically examined some classic philosophical and legal theories of privacy - the non-intrusion, seclusion, limitation, and control theories of privacy. The author argued that each theory falls short of providing an adequate account of privacy. The author further examined and defended a theory of privacy that incorporates elements of the classic theories into one unified theory: the Restricted Access/Limited Control (RALC) theory of privacy and this theory can help us to frame an online privacy policy that is sufficiently comprehensive in scope to address a wide range of privacy concerns that arise in connection with computers and information technology.

**Preserving History, Preserving Privacy: E-Mail, Archival Ethics, And the Law** by Jordon Steele, *Archival Issues,* Vol. 32, No. 2 (2010), pp. 99-109. Published by Midwest Archives Conference. Through this paper, the author has examined legal and

ethical issues surrounding privacy in email. The author makes an attempt to identify legal and ethical parameters that govern archivists when managing electronic correspondence (email) with archival collections.

**Privacy and the Limits of Law** by Ruth Gavison, *The Yale Law Journal*, Vol. 89, No. 3 (Jan., 1980). A path-breaking analysis of the concept of privacy has been presented by the author as well as an account of the reasons why privacy is valuable, and why it has the coherence that justified maintaining it as both a theoretical concept and an ideal.

**Privacy as a Human Right: Sociological Theory** by Katayoun Baghai, *Special Issue: The Sociology of Human Rights,* Vol. 46, No. 5, (October, 2012). this article grounds the polysemic character of privacy drawing on Durkheim, Simmel, and Luhmann and its contingent legal determination in the functional differentiation of social communication systems. It demonstrates a previously overlooked common denominator among privacy conflicts and an emergent principle for their legal resolution with the help of case-law examples from the US Supreme Court and the European Court of Human Rights.

**Privacy in the Digital Age** by Nuala O'Connor, Alethea Lange, and Ali Lange, *Great Decisions,* (2015). Published by: Foreign Policy Association. Authors have presented diverse meanings of privacy before and in the digital age. Further authors have presented Warren & Brandy's concept of privacy as "the right to be let alone" at the time of the invention of the Kodak camera and recent jurisprudence on the topic. Authors have also discussed different kinds of technology involved which violates the privacy of individuals.

**Privacy: Its Meaning and Value** by Adam D. Moore, *American Philosophical Quarterly,* Vol. 40, No. 3 (Jul., 2003). The author has argued that privacy is valuable for everyone. The ability to regulate access to our bodies, capacities, and powers and to sensitive personal information is an essential part of human flourishing or wellbeing. Modern surveillance techniques, data mining efforts, and media coverage are opening up private lives for public consumption. Technological advancements in monitoring and data acquisition are forcing us to rethink our views about the value of privacy.

**Privacy: Philosophical Dimensions** by Ferdinand Schoeman, *American Philosophical Quarterly*, Vol. 21, No. 3 (Jul., 1984). Published by: University of Illinois Press on behalf of the North American Philosophical Publications. The author has explored the nature of privacy with the help of different definitions. Author's

discussion in the article is based on the theme Is privacy coherent and distinctive, Is privacy culturally relative. Further author has critically reviewed the literature available on the topic. The author has further presented the relationship of privacy with individual dignity.

**Protecting Privacy in an Information Age: The Problem of Privacy in Public** by Helen Nissenbaum, *Law and Philosophy,* Vol. 17, No. 5/6 (Nov., 1998). Published by: Springer. This paper has argued for a right to privacy that would encompass privacy in public. Although it does not articulate a theory from which this extended right can be derived, it has advanced principles to guide the development of such a theory, principles according to which activities that, in the past, have fallen outside the scope of many influential legal and philosophical theories, may be judged relevant to a moral right to privacy.

**The current case law of the European Court of Human Rights on privacy: challenges in the digital age** by Özgür Heval Çınar, *The International Journal of Human Rights* (2021). DOI: 10.1080/13642987.2020.1747443. The author has highlighted the right to privacy enshrined in international human rights and shown urgency to protect it from the interference of state and private actors in the private lives of people. The author has especially dealt with a close look at Article 8 of the European Convention on Human Rights, its historical origins, definition, and scope. The article has also examined the current case law of the European Court of Human Rights in light of the current developments in the digital world.

**The Economics of Privacy** by Alessandro Acquisti, Curtis Taylor and Liad Wagman, *Journal of Economic Literature,* Vol. 54, No. 2 (June, 2016). This article is based on theoretical and empirical research on the economics of privacy. Authors have focussed on the economic value and consequences of protecting and disclosing personal information, and on consumers' understanding and decisions regarding the trade-offs associated with privacy and the sharing of personal data. Authors have concluded that characterizing a single unifying economic theory of privacy is hard; in digital economies, consumers' ability to make informed decisions about their privacy is severely hindered because consumers are often in a position of imperfect or asymmetric information regarding when their data is collected, for what purposes, and with what consequences.

**The Four Parts of Privacy in India** by Bhairav Acharya, *Economic and Political Weekly*, Vol. 50, No. 22 (May 30, 2015). Author has presented different

dimensions of privacy in terms of diverse meaning, the traditional theoretical concept of privacy and its protection claimed against other people, society, and the state. The author has further argued that in the context of India, privacy law is evolving in response to four types of privacy claims: against the press, against state surveillance, for decisional autonomy, and in relation to personal information. The Supreme Court has selectively borrowed competing foreign privacy norms, primarily American, to create an unconvincing pastiche of privacy law in India. These developments are undermined by a lack of theoretical clarity and the continuing tension between individual freedoms and communitarian values.

**The Right to Privacy** by Samuel D. Warren & Louis D. Brandeis, *Harvard Law Review,* Vol. 4, No. 5. (Dec. 15, 1890). Authors made efforts to recognize the right to privacy as "the right to be let alone" in the common law first time with the advancement of technology like the inventions of the Kodak Camera. In the beginning, it seemed that authors efforts went in vain but later on their efforts proved mile stone in the history of the right to privacy.

**Understanding Privacy Online: Development of a Social Contract Approach to Privacy** by Kirsten Martin, *Journal of Business Ethics*, Vol. 137, No. 3 (September 2016). The author through this paper explores a social contract approach to developing, acknowledging, and protecting privacy norms. The goal of this paper is to examine how privacy norms develop through the social contract's narrative, to redescribe privacy violations given the social contract approach, and to critically examine the role of business as a contractor in developing privacy norms.

**REPORTS**

**Social Media for Youth & Civic Engagement in India,** published Jointly by Ministry of Youth Affairs & Sports, UNV (United Nations Volunteer India), and UNDP (2019), this report is the outcome of primary field research work conducted across the project intervention districts which reached out to over 1000 young individuals from 15 districts. The report has highlighted that social media has opened a plethora of opportunities for the young people who no longer need a physical space to innovate and initiate action. Social media, if used effectively, has the power to harness the potential of the youth and direct them towards civic engagement.

**Law Commission of India, Srikrishna Committee Report (Data Protection)** The Government of India had set up Committee of Experts with the objective to study

various issues relating to data protection in India, in order to make specific suggestions on principles underlying a data protection bill and draft such a bill. The overall objective was to "ensure growth of the digital economy while keeping personal data of citizens secure and protected." Going through this report the researcher found that a firm legal framework for data protection is the foundation on which data-driven innovation and entrepreneurship can flourish in India. Fostering such innovation and entrepreneurship is essential if India is to lead its citizens and the world into a digital future committed to empowerment, experiment and equal access. This report has helped the researcher in identifying key data protection issues in India and international best practices in the field of Data Protection.

## 1.4. OBJECTIVES OF THE STUDY

(i) To explore the conceptual and theoretical understanding of the right to privacy in a philosophical perspective and its changing dimensions in the digital age.

(ii) To study privacy policies of social media.

(iii) To study privacy as a human right in the digital age.

(iv) To explore the accountability of operators of social networking sites/Apps in preserving the privacy rights of the citizen.

(v) To analyse various international and national laws related to privacy in the digital age.

(vi) To analyse the awareness about legal provisions and privacy policies of social media among students of central universities in Uttar Pradesh.

## 1.5 HYPOTHESIS

- Privacy policies of social media are ambiguous, coercive, and deceptive.
- Inappropriate legislation is hampering the protection of the privacy rights of social media users.
- Awareness regarding legal provisions and privacy policies of social media among the students of central universities in Uttar Pradesh is not adequate

## 1.6 METHODOLOGY

The proposed research work is analytical, exploratory, and empirical in nature. Literature containing provisions of International Instruments of Human Rights, various conventions, national legislation, reports, articles, judicial precedents, and

constitutional provisions regarding privacy has been studied. Privacy policies of social networking sites/Apps of Google, Facebook, Twitter, and their subsidiaries have been analysed. The doctrinal method has been used to explore the concept of privacy as a human right in the digital age in the context of social media. Both primary and secondary data have been used in the research study. Both online communication and personal interaction or contact mode have been adopted for gathering information for empirical study. The random sampling method for the data collection has been used.

### 1.6.1 UNIVERSE OF STUDY

Six central universities namely Aligarh Muslim University, Aligarh (AMU), Babasaheb Bhimrao Ambedkar University, Lucknow (BBAU), Banaras Hindu University, Varanasi (BHU), Rajiv Gandhi National Aviation University, Raebareli (RGNAU), Rani Lakshmi Bai Central Agriculture University, Jhansi (RLBCAU), University of Allahabad, Prayagraj (AU) in Uttar Pradesh has been taken as the universe of the study. Primary data have been collected from the students of these six central universities in Uttar Pradesh.

### 1.6.2 SAMPLE SIZE

A total 600 hundred questionnaires have been filled up by students of six central universities (100 from each university) in Uttar Pradesh.

### 1.6.3 TOOLS AND TECHNIQUES FOR DATA COLLECTION

The data have been collected with the help of both qualitative and quantitative methods. The questionnaire, consisting of 25 different questions has been used to collect primary data of students of six central universities using social media. The researcher sent a structured questionnaire designed in google form to the respondents using social media means like WhatsApp & emails and the researcher also personally contacted respondents, distributed questionnaire, and asked them to fill up the questionnaires. Through persuasion, several verbal reminders, and frequent personal contacts, the researcher has succeeded in getting feedback from 600 respondents. Apart from this, the information from the concerned authorities (six central universities in Uttar Pradesh) has been sought through filing online and offline applications under the provisions of the Right to Information Act, 2005 to know the privacy trends in these universities. Then the obtained data were

processed with the help of statistical tools like Statistical Package for Social Science (SPSS) and MS-Excel.

## 1.7 SIGNIFICANCE OF THE STUDY

- The findings of the research will help social media users to understand the importance of awareness or knowledge related to privacy issues of social media.
- The present study shall enhance the existing knowledge regarding emerging issues of privacy in the digital age.
- The suggestions and findings of the present study may be utilized by law-making authorities and other stakeholders.
- The present study will also strengthen the human rights approach to protect, promote and respect the right to privacy of social media users in India.

## 1.8. LIMITATION OF THE STUDY

As privacy is a broad area, hence present study is focused on informational and communicational privacy. The major social networking sites/Apps namely Google, Facebook, Twitter, and their subsidiaries have been taken into account for analysing privacy policies.

## 1.9 SCOPE FOR FUTURE RESEARCH

The present work is confined to knowing the awareness regarding legal provisions and privacy policies of social media among the students of central universities in Uttar Pradesh as well as to exploring the nature of privacy policies of social networking sites mainly Facebook, Google, Twitter, and their subsidiaries. As today social media is being used by people with different backgrounds irrespective of the location of residence (rural or urban), an education level (highly educated or literate), economic condition (rich or poor), age (old or child), sex (male, female or others). There is a lot of scope for further research on the topic "the right to privacy in the digital age" focussed on women and, children, based on rural areas or other specific groups. A multidisciplinary approach to research is required with a combination of law, Information technology (to know how these technologies - AI, social media, Big Data are developed), Economics, and other fields of social science to minimize the violations of privacy in the digital age.

## 1.10 SCHEME OF CHAPTERS

In order to achieve the objectives of the study, the thesis is divided into seven chapters: -

**Chapter I: INTRODUCTION**

Chapter 1 introduces the subject matter. To make an extensive and comprehensive study of the subject, a brief description reflecting on the objectives of the study, hypotheses/research questions raised, and methodology applied, is the focal point of Chapter 1.

**Chapter II: CONCEPTUAL AND THEORETICAL UNDERSTANDING OF PRIVACY**

Chapter II proceeds to examine the meaning, definitions, conceptual preliminaries, and theoretical exposition of privacy in the traditional and modern spheres in the era of social media.

Apart from the traditional approach of privacy - bodily Privacy, territorial privacy, communication privacy, information privacy, nexus of privacy with data protection, data security, and surveillance in the digital age has been discussed. 'Privacy by Design', 'Privacy by Default', and 'Intellectual privacy' are part of the discussion of this chapter as these are evolving concepts with technological advancement. A conceptual discussion of privacy based on popular concepts 'the right to be let alone', 'limited access to the self', 'secrecy', 'control over personal information, 'personhood', 'intimacy' has been covered in this chapter.

**Chapter III: PRIVACY POLICIES OF SOCIAL MEDIA**

Chapter III contains a systematic analysis of privacy policies of social networking sites /Apps. Efforts have been made to analyze the legality of privacy policies in the light of worldwide recognized data protection principles. Further the researcher has tried to find out the nature of the privacy policies of social networking sites/apps.

Privacy policies of major Social Networking Sites/Apps - Facebook, Twitter, Google, and their subsidiaries have been examined. Ambiguity in the language of privacy policy, targeted advertising, web tracking, not reading privacy policies by social media users, self-regulation mode of operation of social networking sites/Apps, unambiguous consent, how users perceive privacy policies, how users misinterpret

privacy policies and other issues connected with privacy policies have been discussed in this chapter. News Feed, Becon, Facebook Apps, Photo-sharing, Facial Recognition Technology (FRT) controversial features of Facebook have been discussed. How different products namely Google search engine, Gmail, Google Street View, Buzz and Google+ of Google are eroding privacy of individuals is part of discussion of this chapter. Comparative analysis of privacy policies (what kind of data is collected, purpose of collection, sharing of data with others) of Facebook, Twitter and Google has been done.

**Chapter IV: PRIVACY LAWS AND SOCIAL MEDIA: INTERNATIONAL PERSPECTIVE**

Chapter IV is an attempt to discuss in detail the legal framework of privacy laws in the context of social media worldwide. The Organization for Economic Co-operation and Development (OECD) Privacy Guidelines (1980), Data Protection Act of UK 1984, General data protection directive 95/46/EC, UK Data Protection Act, 1984, New EU GDPR and their various provisions applicable to social networking sites/apps have been discussed in this chapter.

Apart from above mentioned statutory provisions applicable to social media, the role of the United Nations in the protection of the right to privacy in the digital age has been examined. United Nations' recommendations to states to take measures to put an end to violations of the right to privacy, review their laws on regular basis, and establish independent, effective machinery to protect the right to privacy is a part of discussion under this chapter. Business enterprises' have been advised to adopt Ruggie's model of "Protect, Respect and Remedy" by the UN.

The chapter concluded by drawing attention to the fact although there is wide and continuous recommendations to protect "the right to privacy in the digital age" by the states as well as business enterprises but there is a huge implementation gap at national level and by the business enterprises.

**Chapter V: PRIVACY LAWS AND SOCIAL MEDIA: NATIONAL PERSPECTIVE**

Chapter V is devoted to legal framework of privacy in context of social media in India. Relevant provisions of Information Technology Act, 2000, Information Technology (Reasonable Practices and sensitive personal information and Procedures) Rules, 2011, Personal Data Protection Bill, 2019, The Information Technology

(Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 applicable to social media with case laws have been discussed.

In this chapter, it is acknowledged that despite all international obligations of India, recommendations given by the United Nations as well as Puttaswamy Constitutional Bench decision to enact data protection law, the Government of India has still a lot of work to be done to achieve the aspirations of these organizations.

**Chapter VI: DATA ANALYSIS AND INTERPRETATION**

Chapter VI contains information about the empirical study area, collection, and analysis of data, interpretation, and results. The purpose of this chapter is to examine, interpret and critically evaluate information gathered from social media users and authorities (central universities in U.P.) to achieve the objectives of the present study. This chapter is the heart of the whole of the research work. Through textual discussion, tabular, and graphs, the data is critically analysed and reported along with the findings.

**Chapter VII: CONCLUSION AND SUGGESTIONS**

The concluding chapter presents the research study with reference to the theoretical analysis, the result obtained from the empirical study, the conclusion arrived and suggestions provided. Further, a few suggestions have also been made to reform the law with respect to the right to privacy in the digital age as well as to spread awareness among the youth of this nation to understand the value of their personal information shared with social networking sites/Apps.

# CHAPTER-II

# CONCEPTUAL AND THEORETICAL UNDERSTANDING OF PRIVACY

# CHAPTER II
# CONCEPTUAL AND THEORETICAL UNDERSTANDING OF PRIVACY

## 2.1 INTRODUCTION

Privacy is an issue of profound importance around the world. With the rise of the Internet and today's interconnected, computerized world has come troubling new threats to privacy and personal information. The whole idea of privacy has changed radically in the digital age. Today many people not only make purchases online using credit card numbers but also share intimate personal details via social media such as Facebook, LinkedIn, and Twitter. Search engines and websites gather and maintain mountains of information about users. Society continues to wrestle with issues of privacy even as new technologies appear every month.

The term "privacy" is used frequently in ordinary language as well as in philosophical, political, and legal discussions, yet there is no universally accepted definition or analysis, or meaning of the term. The concept of privacy is rooted in sociological and anthropological discussions about how extensively it is valued and preserved in various cultures. Moreover, the historical origins of privacy can be traced to philosophical discussions, most notably Aristotle's distinction between the public sphere of political activity and the private sphere associated with family and domestic life. Yet historical use of the term is not uniform, and there remains confusion over the meaning, value, and scope of the concept of privacy.[1]

## 2.2 MEANING OF PRIVACY

Privacy (from Latin Privatus 'separated from the rest, deprived of something, esp. office, participation in the government', from Privo 'to deprive') is the ability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves selectively. The boundaries and content of what is considered private differ among cultures and individuals, but share basic common themes. Privacy is sometimes related to anonymity, the wish to remain unnoticed or unidentified in the public realm. When something is private to a person, it usually means there is something

[1] Stanford Encyclopaedia of Philosophy: Privacy *available at:* https://plato.stanford.edu/entries/privacy/ (last visited on May 30, 2022).

within them that is considered inherently special or personally sensitive. The degree to which private information is exposed therefore depends on how the public will receive this information, which differs between places and over time. Privacy is broader than security and includes the concepts of appropriate use and protection of information.[2]

One of the meanings of the term privacy is the state of being private; retirement or seclusion[3]; the right to be let alone, the right of a person to be free from unwarranted publicity, the right of the individual to withhold himself and his property from public scrutiny, if he so chooses[4]. The other meaning of the term privacy is the quality or state of being apart from company or observation, seclusion, freedom from unauthorized intrusion, place of seclusion, secrecy[5].” The usage of the word “privacy” constitutes the ways in which we employ the word in everyday life and the things we are referring to when we speak of “privacy”. The word “privacy” is currently used to describe a myriad of different things: freedom of thought, control over personal information, freedom from surveillance, protection of one's reputation, protection from invasions into one's home, the ability to prevent disclosure of facts about oneself, and an almost endless series of other things. People can use the word “privacy” improperly by referring to things outside the category or by not referring to things within the category.

## 2.3 DIFFERENT ASPECTS OF PRIVACY

### 2.3.1 BODILY OR PHYSICAL PRIVACY

The most fundamental concern of the concept of rights is concerned with the physical protection of a person. Therefore, the privacy of a person’s physical identity is of vital importance to the foundation of the right to privacy. Bodily privacy is concerned with the protection of one’s physical person – one’s body – against invasive procedures such as drug testing and cavity searches.

The law governing illegal searches and modes of investigation largely addresses the question of bodily privacy in public law. The concern for bodily privacy especially in the area of law enforcement and State action in general is crucial. These instances

[2] *Ibid.*
[3] The Random House Dictionary, (1972).
[4] Black’s Law Dictionary, (1968) at p. 1358.
[5] Webster’s New Collegiate Dictionary (1981) at p. 908.

are evident in daily life which includes searches at airports and investigative techniques such as narco-analysis.

The use of clandestine photography using new technology is now widespread. There have been several instances wherein compromising photographs were taken of persons in public places such as trial rooms and public lavatories. These circumstances cause deep distress and emotional hardship to the victim. Further, in many cases, sensitive data pertaining to an individual's person is divulged to healthcare providers and others. Therefore, there is a pressing need to protect a citizen's person from such attacks on dignity by efficacious criminal and civil remedies.[6]

### 2.3.2 PRIVACY OF HOME AND FAMILY AFFAIRS

The right to privacy traces its origins to the common law dictum of antiquity, "a man's home is his castle". The privacy of the home is one of the most cherished values of a democratic system of rights. The sphere of the State ends at the four walls of a man's home. The privacy of the home is, therefore, inviolable. Territorial privacy concerns the setting of limits on intrusion into the home, workplace, and other geographic or physical locations

Every person has the right to have autonomy in matters of the family. The law must accord protection to the independence of families to determine the manner in which families are formed and continue to live. This includes key aspects of women's rights and reproductive autonomy.[7]

Privacy in sexual relations has also emerged as an import legal issue in this area.

The growth of intrusive journalism in popular media has given rise to a fresh genus of violations of privacy. The augmentation of news media on television and online poses a significant threat to individual privacy and security. This issue is particularly relevant in the case of public figures and celebrities. In the recent past, there has been number of instances of unauthorised photography of homes. In other circumstances, fan club websites constantly update the location and activities of celebrities on their portals endangering security and privacy.[8]

[6] Rishika Taneja and Sidhant Kumar, *Privacy Law Principles, Injunctions and Compensations* 4 (Eastern Book Company, Lucknow, 2014).
[7] *Ibid.*
[8] *Id.* at 5.

The sphere of family life is the most distinguishable aspect of the right to privacy. The right of a person to conduct the affairs of his family in accordance with his personal beliefs and choices is an important facet of privacy.

### 2.3.3 COMMUNICATION PRIVACY

The growth in communication technology is one of the most significant influences on lifestyles and cultures across the globe. It is quite clear that communication privacy has extended beyond telecommunication to the online sphere as well.

Communication privacy covers the security and privacy of mail, telephones, email, and other forms of communication.

In recent years, the extent to which citizens interact by employing means of communication technology has increased manifold. Therefore, there is a pressing need for any privacy framework to cater to the need for communication privacy.[9]

Interception of communication in the current geopolitical environment is often necessary in the interest of national security.

### 2.3.4 INFORMATION PRIVACY

Data and information is an important part of everyday life in today's world. Most transactions are carried out by employing large amounts of this information that may include addresses, financial details, and health records among others.

Informational privacy involves the establishment of rules governing the collection and handling of personal data such as credit information and medical records.[10]

The concept of utilising emerging technologies in the provision of public services and basic governmental processes has gained a great deal of momentum in past few years. The government is slowly but surely evolving into electronic governance models. This necessitates the formation of large public databases that will aggregate large amounts of data which would include data from every facet of a person's life.[11]

There are three popular theories of informational privacy - restricted access theory, the control theory, and the restricted access/limited control theory of privacy.

[9] *Ibid.*
[10] S. R. Chauhan and N.S. Chauhan (eds.), *International Dimensions of the Human Rights* Vol. 2, 689 (Global Vision Publishing House, New Delhi, 2006).
[11] *Supra note* 6 at 6.

The restricted access theory of informational privacy sees privacy achieved if one is able to limit and restrict others from access to personal information. The classical form of this definition is Warren and Brandeis' notion of privacy: "Now the right to life has come to mean the right to enjoy life – the right to be let alone". They discussed this right especially in relation to newspapers and spoke of the "evil of invasion of privacy by the newspapers". The control theory of privacy sees privacy as control and self-determination over information about oneself. Westin provided the most influential control definition of privacy: "Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others". In a control theory of privacy, there is privacy even if one chooses to disclose all personal information about oneself. In an absolute restricted access theory of privacy, there is only privacy if one lives in solitary confinement without contact with others. The restricted access/limited control theory (RALC) of privacy tries to combine both concepts. It distinguishes "between the concept of privacy, which it defines in terms of restricted access, and the management of privacy, which is achieved via a system of limited controls for individuals". All three kinds of definitions of informational privacy have in common that they deal with the moral questions of how information about people should be processed, who shall have access to this data, and how this access shall be regulated. All have in common the normative value that some form of data protection is needed.[12]

## 2.4 CONCEPTUALIZING PRIVACY

The concept of privacy has been used to express variations in the role and scope of a sense of the 'personal' as an autonomous and emancipated sphere. Philosophical traditions and their translation into politics tend to emphasize certain understandings of "privacy." Political and normative dimensions of privacy, as well as regulatory debates about the nature of the right to privacy, its limitations, and possible contexts, demonstrate the centrality and complexity of the concept in the self-imagination and self-governance of human beings and societies. One strong facet of privacy is that of confirming boundaries between an intimate and a more public life for an individual.[13]

[12] Christian Fuchs, *Social Media a critical introduction* 156-157 (Sage Publications India Pvt Ltd, New Delhi, 2017).
[13] Monroe E. Price, Stefaan G. Verhulst, *et.al.* (eds.), *Routledge Handbook of Media Law* 469 (Routledge, New York, 2013).

The philosophical and legal discourse about privacy has proposed numerous conceptions in an attempt to capture the common denominator of privacy. Each of them, however, has significant limitations if it is to serve as a conceptual account.[14]

### 2.4.1 THE RIGHT TO BE LET ALONE

In 1890, Samuel D. Warren and Louis D. Brandeis wrote their famous article "The Right to Privacy," argued for the legal recognition of a right to privacy, which they defined as a "right to be let alone."[15] Many scholars have opined that Warren and Brandeis's article paved the way to lay down the foundation of privacy law in the United States. One has called it the "most influential law review article of all," and another has observed that it "has attained what some might call legendary status." It got popularity as "one of the most brilliant excursions in the field of theoretical jurisprudence."[16]

Warren and Brandeis described how new technological advancements posed a serious threat to privacy. They observed that "[instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life, and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[17] By "instantaneous photographs," they were referring to the new snap cameras invented by Eastman Kodak Company in 1884. Before this invention, photography was largely practiced by professionals, since cameras were large, expensive, and time-consuming to set up. Kodak's new cameras were small and cheap, allowing anybody to become a photographer. In 1889, a year before Warren and Brandeis published their article, photography was so popular that it was referred to in newspapers as a "craze."[18]

Warren and Brandeis were concerned not only with new technology but with how it would intersect with the media. The press was highly sensationalistic at the time. "The press is overstepping in every direction the obvious bounds of propriety and of decency," Warren and Brandeis wrote. "Gossip is no longer the resource of the idle and of the vicious, but has become a trade."[19]

---

[14] Daniel J. Solove, *Understanding Privacy* 14-15 (Harvard University Press, Cambridge, 2008).
[15] Samuel D. Warren, and Louis D. Brandies, "The Right to Privacy" 4 (5) *Harvard Law Review* 193 (1890). Stable URL: https://www.jstor.org/stable/1321160.
[16] Daniel J. Solove, *Understanding Privacy* 15 (Harvard University Press, Cambridge, 2008).
[17] *Supra* note 15 at 195.
[18] Robert E. Mensel, "Kodakers Lying in Wait: Amateur Photography and the Right to Privacy in New York" 43 *American Quarterly* 1885-1915 (1991).
[19] *Supra* note 15 at 196.

Warren and Brandeis while examining the efficacy of contemporary law to protect the privacy of individuals emphasised, "to consider whether the existing law affords a principle which can properly be invoked to protect the privacy of the individual; and, if it does, what the nature and extent of such protection is." The authors argued that a right to privacy could be derived from the common law. Warren and Brandeis defined privacy as the "right to be let alone," a phrase adopted from Judge Thomas Cooley's famous treatise on torts in 1880.[20]

The authors declared that the underlying principle of privacy was "that of an inviolate personality." They noted that the value of privacy "is found not in the right to take the profits arising from publication, but in the peace of mind or the relief afforded by the ability to prevent any publication at all." While the law of defamation protected injuries to reputations, privacy involved "injury to the feelings." Warren and Brandeis argued that the "common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others." This right "the right to be let alone" was a "general right to the immunity of the person, the right to one's personality."[21]

Warren and Brandeis's article, and their conception of privacy as the right to be let alone, profoundly influenced privacy law in the United States. Soon after the article's publication, courts and legislatures began to recognize the right to privacy. The authors' conception of privacy influenced not only tort actions but constitutional and statutory law as well. Indeed, Warren and Brandeis spoke of privacy as a "right," not merely a ground for a tort lawsuit.[22] In 1891, just a year after the article was published, the Supreme Court referred to the right to be let alone in holding that a court could not force a plaintiff in a civil case to submit to a surgical examination: "As well said by Judge Cooley: 'The right to one's person may be said to be a right of complete immunity; to be let alone.'"[23]

[20] *Id.* 15 at 197.
[21] *Ibid.*
[22] David W. Leebron, "The Right to Privacy's Place in the Intellectual History of Tort Law" 41 *Case Western Reserve Law Review* 769, 807-809 (1991).
[23] Union Pac. Ry. Co. v. Botsford, 141 U.S. 250, 251 (1891).

Although Warren and Brandies' work on "The Right to Privacy" had a profound influence on the privacy laws of USA even then it did not remain untouched to criticism. Legal scholar Ruth Gavison stated that the conception of privacy as the right to be let alone, however, fails to provide much guidance about what privacy entails. Understanding privacy as being let alone does not inform us about the matters in which we should be let alone. Warren and Brandeis did speak of "inviolate personality," which could be viewed as describing the content of the private sphere, but this phrase is vague, and the authors failed to elaborate".

Daniel J. Solove argues that 'The right to be let alone' views privacy as a type of immunity or seclusion. As many commentators lament, defining privacy as the right to be let alone is too broad. For example, legal scholar Anita Allen explains, "If privacy simply meant 'being let alone,' any form of offensive or harmful conduct directed toward another person could be characterized as a violation of personal privacy. A punch in the nose would be a privacy invasion as much as a peep in the bedroom." According to philosopher Ferdinand Schoeman, Warren and Brandeis "never define what privacy is." Edward Bloustein, a legal theorist of privacy, observed that instead of developing a conception of privacy, Warren and Brandeis's article focused mostly on the gaps in existing common-law torts.[24]

To its credit, the article was far ahead of its time, and it contained flashes of insight into a more robust theory of privacy. And to be fair, Warren and Brandeis's aim was not to provide a comprehensive conception of privacy but instead to explore the roots of the right to privacy in the common law and explain how it could develop. The article was certainly a profound beginning toward developing a conception of privacy. However, although the right to be let alone has often been invoked by judges and commentators, it still remains a rather broad and vague conception of privacy.[25]

### 2.4.2 LIMITED ACCESS TO THE SELF

Another group of theorists characterize privacy as "limited access" to the self. This conception is based on the individual's desire for concealment and for being apart

[24] *Supra* note 14 at 18.
[25] *Ibid.*

from others. Thus, it is closely related to 'the right to be let alone' conception and is perhaps even a more sophisticated formulation of it.[26]

Sometimes the limited access to self is mistaken as equivalent to solitude. Solitude is a form of seclusion, of withdrawal from other individuals, of being alone. Solitude is a component of limited-access conceptions, as well as of the right-to-be-let-alone conception, but these theories extend far more broadly than solitude, embracing freedom from government interference, as well as from intrusions by the press and others. Limited access conceptions recognize that privacy extends beyond merely being apart from others.[27]

E. L. Godkin, in the late nineteenth century, advanced an early version of the limited access theory when he observed that "nothing is better worthy of legal protection than private life, or, in other words, the right of every man to keep his affairs to himself and to decide for himself to what extent they shall be the subject of public observation and discussion."[28] In July 1890 the same year as the publication of Warren and Brandeis's article, Godkin published an article in which he noted that privacy constituted the "right to decide how much knowledge of his personal thought and feeling, and how much knowledge, therefore, of his tastes and habits, of his own private doings and affairs, and those of his family living under his own roof, the public at large shall have."[29]

Limited-access conceptions have been advanced by several contemporary theorists. Sissela Bok conceives of privacy as "the condition of being protected from unwanted access by others either physical access, personal information, or attention."[30] For Hyman Gross, privacy is "the condition of human life in which acquaintance with a person or with affairs of his life which are personal to him is limited."[31] According to Ernest Van Den Haag, "Privacy is the exclusive access of a person (or other legal entity) to a realm of his own. The right to privacy entitles one to exclude others from (a) watching, (b) utilizing, (c) invading (intruding upon, or in other ways affecting) his

[26] *Ibid.*
[27] *Ibid.*
[28] E. L. Godkin, "Libel and Its Legal Remedy" 12 *Journal of Social Science* 69, 80 (1880).
[29] *Supra* note 14 at 18.
[30] Sissela Bok, *Secrets: On the Ethics of Concealment and Revelation* 10-11 (Pantheon, New York, 1983).
[31] Hyman Gross, "The Concept of Privacy" 43 *New York University Law Review* 34, 35-36 (1967).

private realm."[32] Anita Allen, another legal theorist asserts that "a degree of inaccessibility is an important necessary condition for the apt application of privacy."[33]

Legal scholar David O'Brien argues that there is an important distinction among theorists who conceptualize privacy as limited access formulations. Some view limited access as a choice, a form of individual control over who has access to the self. Others view limited access as a state of existence. Emphasizing on the latter view, O'Brien claims that privacy "may be understood as fundamentally denoting an existential condition of limited access to an individual's life experiences and engagements." "Privacy is not identical with control over access to oneself, because not all privacy is chosen. Some privacy is accidental, compulsory, or even involuntary."[34] For O'Brien, privacy boils down to the condition of being alone. O'Brien's conception, however, omits any notion of the individual's power to make certain choices about revealing aspects of herself to others. For example, O'Brien claims that in a situation of a person stranded on a deserted island has complete privacy, but this is probably better understood as a state of isolation. Privacy involves one's relationship to society; in a world without others, claiming that one has privacy does not make much sense.[35]

Daniel J. Solove argues that without identifying private matters, limited-access conceptions do not tell us the substantive matters for which access would implicate privacy. Solove further asserts that certainly not all access to the self infringes upon privacy, only access relating to specific dimensions of the self or to particular matters and information. The theory provides no understanding as to the degree of access necessary to constitute a privacy violation. Thus, the limited-access conception like *the right to be let alone* conception suffers from being too broad and too vague.[36]

While making an attempt to address these shortcomings, Ruth Gavison develops the most compelling limited access conception. The aim of Gavison is to define "a neutral concept of privacy" that is "distinct and coherent" because "the reasons for which we claim privacy in different situations are similar." Gavison asserts that limited access is the common denominator of privacy: "Our interest in privacy is related to our

[32] *Supra* note 14 at 19.
[33] Edward Shils, "Privacy: Its Constitution and Vicissitudes" 31 *Law and Contemporary Problems* 281, 281 (1966).
[34] David M. O'Brien, *Privacy, Law, and Public Policy* 15-16 (Praeger, New York, 1979).
[35] *Supra* note 14 at 20.
[36] *Ibid.*

concern over our accessibility to others, that is the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of attention of others.'" According to Gavison, privacy cannot be understood "as a claim, a psychological state, or an area that should not be invaded or as a form of control." Unlike many limited access theorists who neglect to elaborate on the value of privacy, Gavison argues that privacy as limited access to the self is valuable in furthering liberty, autonomy, and freedom.[37]

Further, Gavison explains that "three independent and irreducible elements: secrecy, anonymity, and solitude" constitutes limited access.[38] The way that Gavison defines access, however, restricts privacy to matters of withdrawal (solitude) and concealment (secrecy, anonymity). Excluded from this definition are invasions into one's private life by harassment and nuisance and the government's involvement in decisions regarding one's body, health, sexual conduct, and family life.[39] Solove argues that although Gavison contends that "the collection, storage, and computerization of information" falls within her conception, these activities often do not reveal secrets, destroy anonymity, or thwart solitude. Therefore, although Gavison avoids the broadness and vagueness of most limited-access conceptions, her attempt to define what "access" entails winds up being too narrow.[40]

### 2.4.3 SECRECY

One of the most common understandings of privacy is that it constitutes the secrecy of certain matters. Under this view, privacy is violated by the public disclosure of previously concealed information. According to Judge Richard Posner:

The word 'privacy' seems to embrace at least two distinct interests. One is the interest in being left alone - the interest that is invaded by the unwanted telephone solicitation, the noisy sound truck, the music in elevators, being jostled in the street, or even an obscene theatre billboard or shouted obscenity. The other privacy interest, concealment of information, is invaded whenever private information is obtained against the wishes of the person to whom the information pertains.[41]

---

[37] Ruth Gavison, "Privacy and the Limits of Law" 89 (3) *The Yale Law Journal* 423, 426, 433 (Jan., 1980). Stable URL: http://www.jstor.org/stable/795891.
[38] *Ibid.*
[39] *Ibid.*
[40] *Supra* note 14 at 21.
[41] Richard A. Posner, *The Economics of Justice* 272-273 (Harvard University Press, Cambridge, 1981).

The latter privacy interest, "concealment of information," involves secrecy, and Posner defines it as an individual's "right to conceal discreditable facts about himself."[42] Posner sees privacy as a form of self-interested economic behavior, concealing true but harmful facts about oneself for one's own gain. People "want to manipulate the world around them by selective disclosure of facts about themselves."[43] "When people today decry lack of privacy," Posner argues, "what they want, I think, is mainly something quite different from seclusion; they want more power to conceal information about themselves that others might use to their disadvantage."[44] In a less normatively charged manner, psychologist Sidney Jourard emphasizes secrecy in his definition of privacy: "Privacy is an outcome of a person's wish to withhold from others certain knowledge as to his past and present experience and action and his intentions for the future."[45]

Solove argues that the privacy as secrecy conception can be understood as a subset of limited access to the self. He further argues that Secrecy of personal information is a way to limit access to the self. This conception is narrower than limited-access conceptions because secrecy involves only one dimension of access to the self - the concealment of personal facts.[46]

According to Solove, in a variety of legal contexts, the view of privacy as secrecy often leads to the conclusion that once a fact is publicly divulged - no matter how limited or narrow the disclosure - it can no longer remain private. Privacy is thus viewed as coextensive with the total secrecy of information.[47]

Several theorists have claimed that understanding privacy as secrecy conceptualizes privacy too narrowly. Legal theorist Edward Bloustein has criticized the theory of privacy as secrecy as failing to recognize group privacy.[48]

According to Sociologist Amitai Etzioni privacy is "the realm in which an actor (either a person or a group, such as a couple) can legitimately act without disclosure and accountability to others."[49] Nevertheless, even under the selective-secrecy conception,

---

[42] Richard A Posner, *Economic Analysis of Law* 46 (Harvard University Press, Cambridge, 5th edn., 1998).
[43] *Id*. at 234.
[44] *Id.* at 271.
[45] Sidney M. Jourard, "Some Psychological Aspects of Privacy" 31 *Law and Contemporary Problems* 307 (1966).
[46] *Supra* note 14 at 22.
[47] *Ibid.*
[48] Edward J. Bloustein, Individual and Group Privacy 123-186 (Transaction Publishers, New Jersey, 1978).
[49] Amitai Etzioni, *The Limits of Privacy* 196 (Basics Books, New York, 1999).

the harm caused by an invasion of privacy is understood as the disclosure of previously concealed information. Privacy, however, involves more than avoiding disclosure; it also involves the individual's ability to ensure that personal information is used for the purposes she desires.

We have often expectations of privacy even in public. Not all activities we deem private occur behind the curtain. The books we read, the products we purchase, and the people we associate with are often not secrets, but we nonetheless view them as private matters. Philosopher Julie Inness has observed that privacy as secrecy omits the element of control: "Privacy might not necessarily be opposed to publicity; its function might be to provide the individual with control over certain aspects of her life."[50] Similarly, Stanley Benn argues that matters are private not because they "are kept out of sight or from the knowledge of others" but because they "are matters that it would be inappropriate for others to try to find out about, much less report on, without one's consent."[51]

Therefore, although most theorists recognize the disclosure of certain secrets to be a violation of privacy, many commonly recognized privacy invasions do not involve the loss of secrecy. Secrecy as the common denominator of privacy makes the conception of privacy too narrow.

### 2.4.4 CONTROL OVER PERSONAL INFORMATION

The control over personal information theory has got a prominent place in theories of privacy. It has a lot of relevancies in the era of social media where enormous personal information is being disseminated by users online. Several scholars attempt to define privacy in terms of control over personal information. Prof. Allen Westin is the foremost scholars in defining privacy in terms of control over personal information. According to Alan Westin, "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[52] Another scholar, Arthur Miller declares that "the basic attribute of an effective right of privacy is the individual's ability to control the circulation of information relating to him."[53] According to Charles Fried, "Privacy is

[50] Julie Inness, *Privacy, Intimacy, and Isolation* 6 (Oxford University Press, New York, 1992).
[51] Stanley I. Benn, "Privacy, Freedom, and Respect for Persons", in J. Roland Pennock & J.W. Chapman, *et.al. (*eds.), *Privacy: Nomos XIII* 2 (Atherton Press, New York, 1971).
[52] Alan Westin, *Privacy and Freedom* 1 (IG Publishing, New York, 1967).
[53] Arthur Miller, *Assault on Privacy* 25 (The University of Michigan Press, 1971).

not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves."[54]

The control over information conception can be viewed as a subset of the limited-access conception. This theory is not universally accepted, it has some shortcomings likewise other theories of privacy. The first shortcoming is that the theory's focus on information, however, makes it too narrow, for it excludes those aspects of privacy that are not informational, such as the right to make certain fundamental decisions about one's body, reproduction, or rearing of one's children. Secondly, the theory is too vague because it fails to define the types of information over which individuals should have control. For example, Philosopher Ferdinand Schoeman observes that "regarding privacy as a claim or entitlement to determine what information about oneself is to be available to others . . . [wrongly] presumes privacy is something to be protected at the discretion of the individual to whom the information relates."[55] In other words, the control over information conception focuses on all information over which individuals want to retain control, but privacy is not simply a subjective matter of individual prerogative; it is also an issue of what society deems appropriate to protect.

Additionally, some theorists attempt to define the scope of what constitutes personal information over which individuals should exercise control, but their attempts run into significant difficulties. For example, legal scholar Richard Parker's theory covers the scope of personal information arising out of the body's sense organs coming in contact with their objects, extremely broadly: "Control over who can see us, hear us, touch us, smell us, and taste us, in sum, control over who can sense us, is the core of privacy."[56] Other scholars limit the scope of personal information to that which relates to the individual. Richard Murphy, a law and economics scholar, defines the scope of personal information as consisting of "any data about an individual that is identifiable to that individual."[57] Solove argues that Murphy's definition is too broad because there is a significant amount of information identifiable to us that we do not deem as private.

[54] *Supra* note 14 at 20.
[55] Ferdinand David Schoeman, *Philosophical Dimensions of Privacy - An Anthology* 3 (Cambridge University Press, Cambridge, 1984).
[56] Richard B. Parker, *Definition of Privacy* 280 (Routledge, New York, 2001).
[57] Richard S. Murphy, "Property Rights in Personal Information: An Economic Defense of Privacy" 84 *Georgetown Law Journal* 2381, 2383 (1996).

In addition to failing to adequately define the scope of information, control over information conceptions fail to define what is meant by "control." Theory needs to be elaborated further on what control really entails, and it is often defined too narrowly or too broadly. Frequently, control is understood as a form of ownership of information. For example, Westin concludes that "personal information, thought of as the right of decision over one's private personality, should be defined as a property right."[58] This notion is partially embodied in the tort of appropriation, which protects people against others' using their image or likeness for commercial gain.[59]

John Locke's contribution to the development of the notion that individuals have a property right in information about themselves is significant, who asserted that individuals have property rights in their person and the fruits of their labour. According to John Locke, property flows naturally from selfhood: "Every man has property in his own person. This nobody has a right to, but himself." From this principle, Locke deduced that property extends to the products of one's labour: "Whatsoever then he removes out of the state that nature hath provided, and left it in, he hath mixed his labour with, and joined it to something that is his own, and thereby makes it his property."[60]

Today's Intellectual Property Law is based on Locke's conception of property as the fruit of labour and as an extension of the self, which, as legal theorist James Boyle has observed, has developed around the notion of the "romantic author," the individual who mixes her unique personality with ideas, who most displays originality and novelty in her creations.[61] Unlike physical property, intellectual property protects the expression of ideas. Copyright law, for example, protects "original works of authorship fixed in any tangible medium of expression."[62] Copyright law provides control not over the underlying ideas and facts but over the particular manner in which they are expressed. The "romantic-author" notion of intellectual property embodies Locke's idea that one gains a property right in something when it emanates from one's self.

The conception of personal information as property is justified by viewing it as an extension of personality. As we the authors of our own lives, we generate information

[58] *Supra* note 52 at 324.
[59] *Supra* note 14 at 26.
[60] *Ibid.*
[61] James Boyle, *Shamans, Software, and Spleens: Law and the Construction of the Information Society* 54 (Harvard University Press, Cambridge,1996).
[62] U.S. Code 17 (1994), §102 (a).

as we develop our personalities. The growth of individualism spawned the "belief that one's actions and their history 'belonged' to the self which generated them and were to be shared only with those with whom one wished to share them."[63] "One's self for other people - is one's expression of one's self," observes Madame Merle in Henry James's The Portrait of a Lady, "and one's house, one's furniture, one's garments, the books one reads, the company one keeps - these things are all expressive."[64]

Extending property concepts to personal information, however, has some shortcomings. Information can be easily transmitted and, once known by others, cannot be eradicated from their minds. Unlike physical objects, information can be possessed simultaneously within the minds of millions. This is why intellectual property law protects particular tangible expressions of ideas rather than the underlying ideas themselves. The complexity of personal information is that it is both an expression of the self and a set of facts - a historical record of one's behaviour.

Further, there are problems with viewing personal information as equivalent to any other commodity. Personal information is often formed in relationships with others. All parties to that relationship have some claim to the information. For example, according to Jerry Kang, individuals are not the lone creators of their web-browsing information, for most of that information is created from the interaction between the user and websites.[65] Often, the market value of information is not created exclusively by the labour of the individual to whom it relates but in part by the third party that compiles the information.[66] For instance, the value of personal information for advertisers and marketers emerges in part from their consolidation and categorization of that information.

An example of the difficulty in assigning ownership to information is illustrated by Haynes v. Alfred A. Knopf Inc.[67] This case involved Nicholas Lemann, a journalist who wrote a book titled "The Promised Land: The Great Black Migration and How It changed America," which was published by Alfred A. Knopf Inc. The book depicted life sketches of Ruby Lee Daniels, who suffered greatly from her former husband Luther

[63] Edward Shils, "Privacy: Its Constitution and Vicissitudes" 31 *Law and Contemporary Problems* 290 (1996).
[64] Geoffrey Moore (ed.), *Henry James, The Portrait of a Lady* 253 (Penguin Books, London, 1986).
[65] Jerry Kang, "Information Privacy in Cyberspace Transactions", 50 *Stanford Law Review* 1193, 1202, 1246 (1998).
[66] Arthur Miller, *Assault on Privacy* 213 (The University of Michigan Press, 1971).
[67] Haynes v. Alfred A. Knopf, Inc. (1993) - 8 F.3d 1222 (7th Cir. 1993).

Haynes's alcoholism, selfishness, and irresponsible conduct. Plaintiff husband Haynes sued the author and the publisher under the public disclosure of private facts tort, claiming that he had long since turned his life around and that the disclosure of his past destroyed the new life, he had worked so hard to construct. Learned Judge Posner concluded that there could be no liability for invasion of privacy because "a person does not have a legally protected right to a reputation based on the concealment of the truth"[68] and because the book narrated "a story not only of legitimate but of transcendent public interest."[69]

Solove comments that although this case did not hinge on the shared nature of the information, it illustrates that personal information rarely belongs to just one individual; it is often formed in relationships with others. Ruby Daniels's story was deeply interwoven with Haynes's story. Daniels had a right to speak about her own past, to have her story told. This was her life story, not just Luther Haynes's. Solove concludes that understanding control as ownership presents difficulties in grappling with the unique shared nature of much private information. A claim of privacy is not the same as a claim of ownership.[70]

Not only does defining control prove difficult, but also control over information is too broad a conception. Professor Tom Gerety claims that control over information conceptions include "all control over all information about oneself, one's group, one's institutions. Surely privacy should come, in law as in life, to much less than this."[71] According to Inness, not all personal information is private; she asserts that "it is the intimacy of this information that identifies a loss of privacy."[72] Thus one possibility is that the control over information conception could be limited in scope by including only intimate information. Charles Fried seeks to limit his control over information conception in this manner, defining privacy as "control over knowledge about oneself" that is necessary to protect "fundamental relations" of "respect, love, friendship, and trust."[73] His theory speaks about the value of privacy (promoting respect, love, friendship, and trust) and presumably would define the scope of information as

[68] *Ibid.*
[69] *Ibid.*
[70] *Supra* note 14 at 27.
[71] Tom Gerety, "Redefining Privacy" 12(2) *Harvard Civil Rights-Civil Liberties Law Review* 262-263 (1977).
[72] *Supra* note 50 at 58.
[73] Charles Fried, "Privacy" 77 (3) *The Yale Law Journal* 483, 477 (1968).

"intimate" information (information necessary to form and foster relationships involving respect, love, friendship, and trust).

Even if the conception is narrowed to include only intimate information, however, it is still too broad. According to DeCew, we often lose control over information in ways that do not involve an invasion of our privacy.[74] To illustrate this point, Daniel Farber invokes the example of the flasher. A flasher is controlling visual access to his body by allowing it, but preventing flashing is not a violation of the flasher's privacy; rather, flashing is seen as a violation of the privacy of others.[75] David O 'Brien also criticizes the conception of privacy as the control of information for being too narrow.[76] Many privacy interests involve an individual's "freedom to engage in private activities" rather than the disclosure or nondisclosure of information.[77] O 'Brien correctly recognizes that privacy is invaded not just by the loss of control over information but also by nuisances such as noises, smells, and other noxious disruptions of one's peace of mind.[78] DeCew points out that the control over information conception is too narrow because privacy does not involve only personal information. Privacy, contends DeCew, can be invaded even if nobody else knows something new about a person. Examples include being forced to hear propaganda, being manipulated by subliminal advertisements, or being disrupted in a manner that thwarts one's ability to think or read.[79] Anita Allen critiques the control over information conception for omitting issues such as abortion and sexual freedom.[80] The theory of privacy as control over information thus excludes many aspects of life that we commonly assume to be private.

To summarize, conceptualizing privacy as control over personal information can be too vague, too broad, or too narrow. Conceptions of information control are too vague or too broad when theorists fail to define what "control" entails. Attempts to define control often delineate it as a form of ownership, making the conception falter in a

[74] Judith Wagner DeCew, *In Pursuit of Privacy - Law, Ethics, and the Rise of Technology* 53 (Cornell University Press, New York, 1997).
[75] Daniel A. Farber, "Book Review: Privacy, Intimacy, and Isolation by Julie C. Inness," 10 *Constitutional Commentary* 510, 514-15 (1993).
[76] David M. O'Brien, *Privacy, Law, and Public Policy* 13 (Praeger, New York, 1979).
[77] *Ibid.*
[78] *Ibid.*
[79] Judith Wagner DeCew, *In Pursuit of Privacy - Law, Ethics, and the Rise of Technology* 2 (Cornell University Press, New York, 1997).
[80] Anita L. Allen, *Uneasy Access*: *Privacy for Women in a Free Society* 8 (Rowman & Littlefield Publishers, New Jersey, 1988).

number of respects. Finally, conceptions of information control are too narrow because they reduce privacy to informational concerns, omit decisional freedom from the realm of privacy, and focus too exclusively on individual choice.

### 2.4.5 PERSONHOOD

Another theory of privacy views it as a form of protecting personhood. The term "personhood" was coined by Paul Freund to refer to "those attributes of an individual which are irreducible in his selfhood."[81] This term is based on Warren and Brandeis's notion of inviolate personality.

Personhood theory of privacy differs from the theories discussed earlier because it is constructed around a normative end of privacy, namely, the protection of the integrity of personality. This theory is not independent of the other theories, and it often is used in conjunction with them to explain why privacy is important, what aspects of the self should be limited, or what information we should have control over.

Edward Bloustein asserted that privacy protects individuality.[82] Privacy is a unified and coherent concept protecting against conduct that is "demeaning to individuality," "an affront to personal dignity," or an "assault on human personality."[83] Jeffrey Reiman recognizes a personhood component to privacy: "The right to privacy protects the individual's interest in becoming, being, and remaining a person."[84]

Philosopher Stanley Benn also develops a personhood conception of privacy, noting that privacy amounts to respect for individuals as choosers: "Respect for someone as a person, as a chooser, implies respect for him as one engaged in a kind of self-creative enterprise, which could be disrupted, distorted, or frustrated even by so limited an intrusion as watching." Drawing from Jean-Paul Sartre's *Being and Nothingness*, Benn explains that being "an object of scrutiny, as the focus of another's attention, brings one to a new consciousness of oneself, as something seen through another's eyes." The observed "becomes aware of himself as an object, knowable, having a determinate character." According to Benn, the result is that the observed person "is fixed as something — with limited probabilities rather than infinite,

[81] *Supra* note 14 at 29.
[82] *Supra* note 14 at 30.
[83] *Ibid*.
[84] Jeffrey H. Reiman, "Privacy, Intimacy, and Personhood", in Ferdinand David Schoeman, e*t.al.* (eds.), *Philosophical Dimensions of Privacy An Anthology* 300, 314 (Cambridge University Press, 2009).

indeterminate possibilities."[85] In other words, Benn contends that surveillance restricts an individual's range of choices and thus limits her freedom. Accordingly, privacy is about respect for personhood, with personhood defined in terms of the individual's capacity to choose.

Theories of privacy as personhood, however, fail to elucidate what privacy is because they often do not articulate an adequate definition of personhood. Freund's notion of attributes irreducible in one's selfhood is far too vague and merely substitutes "selfhood" for "personhood." Bloustein's discussion of personhood as "individuality" fails to define the scope or nature of individuality. Other commentators define personhood as a type of autonomy,[86] but as legal scholar Jed Rubenfeld observes, "to call an individual 'autonomous' is simply another way of saying that he is morally free, and to say that the right to privacy protects freedom adds little to our understanding of the doctrine."[87]

Personhood theories are often too broad. Our personalities are not purely private; indeed, we readily express in public much that is unique to the self. An artistic work is frequently an expression of the deepest recesses of an artist's existence, yet it is often put on public display. Gavison, for example, criticizes Bloustein's dignity conception because "there are ways to offend dignity and personality that have nothing to do with privacy." She elaborates: "Having to beg or sell one's body in order to survive are serious affronts to dignity, but do not appear to involve loss of privacy."[88]

Jed Rubenfeld in his influential article "The Right of Privacy," has provided a sophisticated account of the problems of the personhood theory of privacy. According to Rubenfeld, the "personhood thesis is this: where our identity or self-definition is at stake, there the state may not interfere." Rubenfeld correctly observes that the law cannot protect all forms of self-definition, for some forms conflict with others, and very few meaningful acts of self-definition have no effects on others. "Personhood cannot exclude 'intolerant' identities without abandoning its value-neutrality as between identities." This fact leads Rubenfeld to conclude that personhood's "final defence"

[85] *Supra* note 51.
[86] Joel Feinberg, "Autonomy, Sovereignty, and Privacy: Moral Ideas in the Constitution?" 58 *Notre Dame Law Review* 445 (1983).
[87] Jed Rubenfeld, *"The Right of Privacy,"* 102 *Harvard Law Review*, 750 (1989).
[88] Ruth Gavison, "Privacy and the Limits of Law" 89 (3) The Yale Law Journal 438 (Jan., 1980). Stable URL: http://www.jstor.org/stable/795891.

rests on a view of what is fundamentally important to individual identity.[89] Rubenfeld then critiques the personhood conception: "By conceiving of the conduct that it purports to protect as 'essential to the individual's identity,' personhood inadvertently reintroduces into privacy analysis the very premise of the invidious uses of state power it seeks to overcome."[90] When the state endeavours to protect personhood, it must adopt and enforce its own conception of individual identity, impinging upon the freedom of individuals to define for themselves what is central to their identities.

Rubenfeld offers an alternative conception that defines the right to privacy as "the fundamental freedom not to have one's fife too totally determined by a progressively more normalizing state." Rubenfeld claims that privacy protects against a "creeping totalitarianism, an unarmed occupation of individuals' lives." Privacy "is to be invoked only where the government threatens to take over or occupy our lives — to exert its power in some way over the totality of our lives." Rubenfeld elaborates: "The anti-totalitarian right to privacy . . . prevents the state from imposing on individuals a defined identity."[91]

Rubenfeld's critique of personhood forbids him from sketching any conception of identity that the law should protect, for to do so would be to seize from individuals their right to define themselves. By abandoning any attempt to define a conception of identity, Rubenfeld's conception of privacy collapses into a vague right to be let alone. For it to tell us anything meaningful about which exercises of state power must be curtailed, a theory of privacy must have an affirmative conception of personhood. For example, Rubenfeld states, "[Childbearing, marriage, and the assumption of a specific sexual identity are undertakings that go on for years, define roles, direct activities, operate on or even create intense emotional relations, enlist the body, inform values, and in sum substantially shape the totality of a person's daily life and consciousness."[92] Rubenfeld defines these aspects of life as existing at the heart of identity because of their pervasiveness and longevity. Thus, he is creating a conception of personhood that focuses on pervasiveness and longevity as the defining factors.

Rubenfeld is correct that laws purporting to protect personhood can impose a view of what aspects of life are essential to the individual and hence supplant the

[89] Jed Rubenfeld, "Right of Privacy" 102 (4) *Harvard Law Review* 773, 754, 758, 770 (1989).
[90] *Ibid.*
[91] *Ibid.*
[92] *Ibid.*

individual's own self-definition. However, Rubenfeld is too quick to condemn as "invidious" all state power that shapes identities.[93] Not all such exercises of state power are pernicious. In fact, privacy is both a positive and a negative right; it is not just a freedom from the state, but also a duty of the state to protect certain matters via property rights, tort law, criminal law, and other legal devices. Without protection against rape, assault, trespass, and the collection of personal information, we would have little privacy and scant space or security to engage in self-definition. To preserve people's ability to engage in self-definition, the state must actively intervene. Therefore, although Rubenfeld is correct that the state cannot be neutral when it becomes involved in one's self-definition, he errs in assuming that he can develop his theory of anti-totalitarianism without an account of personhood.

### 2.4.6 INTIMACY

An increasingly popular theory understands privacy as a form of intimacy. This theory appropriately recognizes that privacy is essential not just for individual self-creation, but also for human relationships. Daniel Farber notes that one virtue of privacy as intimacy is that it "expands moral personhood beyond simple rational autonomy."[94] The theory views privacy as consisting of some form of limited access or control, and it locates the value of privacy in the development of personal relationships.

We form relationships with differing degrees of intimacy and self-revelation, and we value privacy so that we can maintain the desired levels of intimacy for each of our varied relationships. For example, political scientist Robert Gerstein claims that "intimate relationships simply could not exist if we did not continue to insist on privacy for them."[95] By focusing on the relationship-oriented value of privacy, the theory of privacy as intimacy attempts to define what aspects of life we should be able to restrict access to, or what information we should be able to control or keep secret.

Julie Inness in her book titled 'Privacy, Intimacy, and Isolation' advances an intimacy conception of privacy:

[93] *Ibid.*
[94] *Supra* note 14 at 34.
[95] *Ibid.*

*"The content of privacy cannot be captured if we focus exclusively on either information, access, or intimate decisions because privacy involves all three areas. I suggest that these apparently disparate areas are linked by the common denominator of intimacy - privacy's content covers intimate information, access, and decisions."*

According to Inness, "Intimacy stems from something prior to behaviour." It is an individual's motives that matter. Intimate matters or acts draw "their value and meaning from the agent's love, care, or liking." This, she claims, defines the scope of intimacy. Privacy is "the state of the agent having control over decisions concerning matters that draw their meaning and value from the agent's love, caring, or liking. These decisions cover choices on the agent's part about access to herself, the dissemination of information about herself, and her actions."[96]

According to Charles Fried, "Intimacy is the sharing of information about one's actions, beliefs or emotions which one does not share with all, and which one has the right not to share with anyone. By conferring this right, privacy creates the moral capital which we spend in friendship and love."[97] Another scholar James Rachels in a similar manner contends that privacy is valuable because "there is a close connection between our ability to control who has access to us and to information about us, and our ability to create and maintain different sorts of social relationships with different people."

For Fried and Rachels, intimate information is that which individuals want to reveal only to a few other people. Jeffrey Reiman argues that Fried and Rachels's view of intimacy "overlooks the fact that what constitutes intimacy is not merely the sharing of otherwise withheld information, but the context of caring which makes the sharing of personal information significant."[98]

Tom Gerety's formulation of privacy is also based on intimacy. He criticizes that existing theories of privacy are far too broad because they lack any meaningful limitation in scope, he goes on to claim that "intimacy is the chief restricting concept in the definition of privacy." Intimacy is "the consciousness of the mind in its access to its own and other bodies and minds, insofar, at least, as these are generally or specifically secluded from the access of the uninvited." In other words, his definition of intimacy is a form of limited access to the self. Gerety develops his definition of intimacy a bit

[96] *Supra* note 50.
[97] *Supra* note 14 at 35.
[98] *Ibid.*

further in terms of its expressiveness of individual identity and autonomy. He thus claims that abortion is a private decision because it is "an intimate one, expressive of both - a woman's identity and her autonomy."[99]

But Gerety's intimacy theory of privacy, like the theories he critiques, is too broad. Gerety attempts to limit privacy by the terms "identity" and "autonomy," but these very broad terms could apply to almost every action or decision an individual undertakes. While Gerety complains about overbroad conceptions of privacy that have no meaningful limitation, his conception suffers from the same defect. Without limitations in scope, the word "intimacy" is merely a different word for "privacy" and is certainly not sufficient to determine which matters are private.

On the other hand, privacy as intimacy theories are too narrow because they focus too exclusively on interpersonal relationships and the particular feelings engendered by them. Although trust, love, and intimacy are facilitated by privacy, these are not the sole ends of privacy. As DeCew points out, information about our finances is private but not intimate.[100] Trust, love, and caring are not broad enough to constitute a conception of privacy. Although privacy helps us achieve these ends, these ends do not compose a complete conception of privacy. As Farber notes, there are many sexual relationships devoid of love, liking, or caring, and there are many acts expressive of love, liking, or caring (such as buying gifts) that are not considered intimate.[101]

Furthermore, privacy's value does not lie exclusively in the development of intimate human relationships. Intimacy captures the dimension of private life that consists of close relationships with others, but it does not capture the dimension of private life that is devoted to the self alone.

W. L. Weinstein observes:

*[T]here is a wide range of instances where to speak of something as private is not to imply intimacy. Individuals not intimately related may nevertheless assert that their relation or activity is a private one in the sense that it is not the proper concern of the community or some institution, such as the state, a church, or a business firm*.[102]

[99] *Ibid.*
[100] *Ibid.*
[101] *Ibid.*
[102] *Supra* note 14 at 37.

For example, as political scientist Priscilla Regan notes, computer databases pose a significant threat to privacy but "do not primarily affect relationships of friendship, love, and trust. Instead, these threats come from private and governmental organizations — the police, welfare agencies, credit agencies, banks, and employers."[103]

In sum, privacy as intimacy conceptions can be too broad if they do not adequately define the scope of "intimacy." Most often, however, these conceptions are too narrow because they exclude many matters that do not involve the characteristics of intimate relationships.

## 2.5 DEFINING PRIVACY BY INDIAN SCHOLARS

The Indian scholars,[104] who have written articles on privacy, have preferred to rely upon the definition given by the western scholars rather than contributing their own. Shriniwas Gupta, of course, initiated the question regarding the concept of privacy in India but concluded with the following observations:

*Our ancient law in Dharmshashtras also recognised the concept of privacy. Really, the law of privacy has been well-expounded in the commentaries of the old law. Kautilya in his Arthashastra has prescribed a detailed procedure to ensure the right to privacy while ministers were consulted. But neither in ancient law nor in the present law the term 'privacy' has anywhere been defined nor any judicial pronouncement has so far come to make the position clear.*[105]

Pannalal Dhar says that the right to privacy is a right whose contours still remained undefined.[106] Professor P.K. Tripathi relates the right to privacy with the idea of exclusion. To exclude others has remained by and large, the main theme of privacy.

Govind Mishra defines privacy as a fundamental right of the citizens to exclude governmental acts, omissions and things which tend to annoy or embarrass them and which affect the promotion and maintenance of their dignity.[107] However, it is not an exhaustive one. He accepts that privacy is a culturally limited concept.

---

[103] *Ibid*.
[104] Kiran Deshta, *Right to Privacy under Indian Law* 30 (Deep & Deep Publications Pvt. Ltd., New Delhi, 2011).
[105] *Ibid.*
[106] *Ibid.*
[107] *Id.* at 31.

But surprisingly enough, Professor Upendra Baxi has raised a very basic question as to whether 'privacy' is a value of human relations in India. He observes:

*But the question arises at a more general level whether privacy is a value of human relations in India. [Everyday experience in Indian setting suggests otherwise, Marriage parties and midnight music, wedding processions and morning 'bhajans' unabated curiosity at other people's illness or personal vicissitudes, manifestation of good neighbourliness through constant surveillance by the next door neighbour (large number of Indian houses do not use curtains) are some of the common experiences. A question may arise whether privacy is not after all a value somewhat alien to Indian culture.*[108]

There are many other scholars who have also subscribed to the opinion expressed by Professor Baxi.[109]

## 2.6 PRIVACY IN THE COMMON LAW

Privacy was very much in the air in 1890, as elites like the Warrens felt the threat to their social position posed by a new generation of newspaper reporters. Writing for the newly affluent middle classes and armed with new cameras that could take pictures simultaneously, the "Yellow Press" blurred settled lines between public and private. In July, E. L. Godkin, editor of the *The Nation,* argued that the rise of the Yellow Press required a great protection for what he called "the right to privacy." This was a person's right "to decide how much knowledge of his personal thought and feeling, and how much knowledge, therefore, of his tastes and habits, of his own private doings and affairs, and those of his family living under his own roof, the public at large shall have.".[110]

Godkin's essay was part of a wave of privacy anxiety sweeping the Gilded Age's upper classes. Some of their concern was technological. Innovations like the new portable camera allowed photography almost anywhere, not just in the controlled studios of professional photographers.[111]

[108] *Ibid.*
[109] Sir Zelman Cowan, Justice V.R. Krishna Iyer, Sri V.N. Gadgil, M.P. and Mr. Ranjit Lai, a journalist.
[110] Richards, Neil, *Intellectual Privacy Rethinking Civil Liberties in the Digital Age* 16 (Oxford Press, New Delhi, 2015).
[111] *Id.* at 17.

Encouraged by Mabel, Warren sought out Brandies to write an article about the excess of the press and the need for a legal right to privacy. Warren and Brandies worked together on their article through the summer of 1890, and the fruits of their labour were published in the *Harvard Law Review* as *The Right to Privacy* in December. The essay argued that the common law should protect a right to privacy. It came to define not just the field of privacy law but also popular understandings of what privacy means.[112]

A lot has been written about *The Right to Privacy,* but three choices – (1) chose to focus on emotional harm, (2) targeted the press and public debate, and (3) urged courts to police a line between what was fit for the public to know and what was not; Warren and Brandies made in building their argument affected the story of tort privacy in American law.

### 2.6.1 EMOTIONAL HARM

Mabel Warren's goal was to protect elites against *emotional harm* – specifically the publication of private facts and photographs that produced hurt feelings. Traditionally, the common law had rejected claims of emotional injury and had required plaintiffs to prove physical or property injuries before they could recover damage.

### 2.6.2 TARGETING THE PRESS

The second importance choice that Warren and Brandies made in defining the right to privacy was to target the press. Newspapers were the primary source of the invasions of privacy they decried, and newspapers were the intended defendants in the lawsuits they wanted courts to recognize.[113]

Warren and Brandies argued that although verbal gossip was harmful, gossip by journalists was much more dangerous because it was widely circulated and embodied in print. Worse still, they argued, the gossip trade by newsmen was causing "the lowering of social standards of morality." [114]

By crowding out more serious and important information in the minds of citizens, gossip journalism lowered social standards and encouraged "the weak side of human

[112] *Supra* note 15.
[113] *Supra* note 15 at 195.
[114] *Supra* note 111 at 19.

nature" to flourish. Protecting privacy was thus essential to safeguarding not just hurt feelings but the sanctity of public discourse itself.[115]

### 2.6.3 "PUBLIC" AND "PRIVATE"

Warren and Brandies recognized the tension between a right of privacy and a free press and tried to solve this problem by relying on a distinction between the "public" and "private" spheres. They suggested that courts could separate "private" facts from "public" facts, with the press entitled to publish only the latter. The proposed privacy tort would protect only facts "concern[ing] the private life, habits, acts, and relations of an individual." It would not "prohibit any publication of matter which is of public or general interest," allowing, for example, the publication of information with a "legitimate connection" with the fitness of a candidate for public office or any actions taken in the public sphere.[116]

Warren and Brandies admitted that the line between public and private was a fuzzy one, and conceded that they had provided only a rough sketch to guide courts. But they were confident that the courts in the future could develop a better picture of what the public had no right to know. Future courts should recognize, they suggested, that "[s]ome things all men alike are entitled to keep from popular curiosity, whether in public life or not, while others are only private because the persons concerned have not assumed a position which makes their doing legitimate matters of public investigations." [117]

### 2.6.4 THE RISE OF TORT PRIVACY

At first it seemed as if the Warren and Brandies article would, like almost scholarly papers, have no effect on the law. A few early cases almost immediately toyed with the idea of protecting privacy through law, and California enacted a short-lived and effective privacy law in 1899, but it took over a decade for privacy to take serious root.[118] In fact, courts only began to protect against the disclosure of private facts in earnest in the 1920, more than thirty years after the publication of the *The Right to Privacy.*[119] *(Brents v. Morgan case* 1927).

---

[115] *Supra* note 15 at 216.
[116] *Ibid.*
[117] *Ibid.*
[118] *Supra* note 111 at 21.
[119] *Id.* at 23.

But Privacy entered the mainstream of American law because of efforts of Professor William Prosser, dean of the law school at Berkeley and the leading authority on tort law of his day. If Warren and Brandies gave tort privacy its name and guiding principles, Prosser gave it form and credibility. His principal contribution was to argue that the case adopting the Warren and Brandies formulation were not one tort but really "four distinct kinds of invasion of four different interests of the plaintiff, which are tied together by a common name, but otherwise have nothing in common except that each represents an interference with the right of the plaintiff, in the phrase coined by Judge Cooley, 'to be let alone.' Prosser described his four torts as follows:

1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
2. Public disclosure of embarrassing private facts about the plaintiff.
3. Publicity which places the plaintiff in a false light in the public eye.
4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.

   Courts recognized this way of organizing the law, and it has become the foundation of modern tort privacy.[120]

Today the four privacy torts remain on the books much as *Prosser* left them at his death in 1972 – intrusion, disclosure, false light, and appropriation. But virtually all states now recognize some or all of the four Prosser privacy torts.[121]

**INTRUSION –** Intrusion upon seclusion is what we classically think of as invasion of privacy – the violation of a person's private space. The tort requires as intentional intrusion "upon the solitude or seclusion of another or his private affairs or concerns" that is highly offensive to a reasonable person.[122]

**DISCLOSURE –** Publicizing information about the private life of another person may be considered as invasion of privacy if the information is not a matter of legitimate public concern and its publication would be highly offensive to a reasonable person.[123]

[120] William Prosser, *Privacy,* 48 CALIF, L. REV. 383, 406-407 (1960).
[121] Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy,* 98 Calif. L. Rev. 1887, 1893-94 (2011).
[122] Ashley Packard, *Digital Media Law* 260 (John Wiley & Sons, Inc UK, 2013).
[123] *Ibid.*

**FALSE LIGHT –** Publishing information that creates a false impression about someone, thereby casting the person in a false light, constitutes an invasion of privacy in many states. False light bears a resemblance to defamation because both torts involve deliberate misrepresentations. However, false light claims are based on the emotional harm cause by misrepresentation, rather than harm to reputation.[124]

**APPROPRIATION –** Appropriation, the oldest invasion of privacy tort, is committed when someone "appropriates to his own use or benefit the name or likeness of another".[125] As a privacy right, appropriation protects individuals from the emotional distress or embarrassment that might result from having their name or likeness used in an advertisement without their permission.

## 2.7 DEFINING PRIVACY IN THE MODERN SPHERE

The concept of privacy is not amenable to precise definition. In public law, traditionally 'privacy' means freedom from official intrusion. However, today with the development of science and technology and other pressures, the term privacy has received extended meaning.

### 2.7.1 PRIVACY AND DATA PROTECTION

In terms of how we view privacy in modern terms, 'data protection' appeared. Europe as an answer to the dangers of electronic data processing, which were becoming widespread via the time of the so-called electronic revolution, which began in the 1970s. This resulted in the first generation of data protection laws, developed in response to computer systems and the ability to create mass databases from which it was possible to collate and match data through the use of indexing and search engines performed on the basis of keyword searches. At the same time, the appearance of international computer networks opened the road for globalization of data processing as well. The content of the legal protection provided by it has changed significantly since its appearance several times, and is still changing presently as technological advances become increasingly sophisticated.

In the modern age while following on from early definitions, data protection is a tool of privacy protection, and as such is aimed necessarily at the individual; the object of

[124] *Id.* at 269.
[125] *Id.* at 265.

data security is data itself. This may be interpreted as the protection of the integrity and confidentiality of data, irrespective of the information content qualification of data.[126]

### 2.7.2 INTERRELATIONSHIP WITH DATA SECURITY

Data security is served by technical and organizational measures, which may be stipulated both by legal and extra-legal norms. Data security regulations are applied by several legal norms, including the legal formulation of data security regulations concerning qualified data (secrets of State and intelligence). The interrelationship between data protection and data security is complex, although there are certain key features that assist with understanding the nature of the connectivity of security and privacy. Throughout the development of data protection laws, post 1970, although to a variable extent, legislation has usually contained data security rules serving data protection (which give specifications of the technical, organizational or other measures that are to be followed by the addressee of the norm when treating personal data). Such measures indicate that with regard to personal data, data security is of the objectives of data protection regulation.[127]

A new development among the tools of privacy protection is the increasing role of data security technologies; this has been especially marked over the past few years, which has seen increased focus on users' sophistication with the development of computer technology.[128]

### 2.7.3 PRIVACY AND SURVEILLANCE

In modern society, privacy is inherently linked to surveillance. Based on Foucault's notions of surveillance as disciplinary power, one can define surveillance as a specific kind of information gathering, storage, processing, assessment and use that involves potential or actual harm, coercion, violence, asymmetric power relations, control, manipulation,[129] domination or disciplinary power. Surveillance is instrumental and a means for trying to derive and accumulate benefits for certain groups or individuals at the expense of other groups or individuals. Surveillance is based on the logic of competition. It tries to bring about or prevent certain behaviours of groups

[126] Laura Scaife, *"Handbook of Social Media and the Law* 240 (Informa Law from Routledge, New York, 2015).
[127] *Ibid*.
[128] *Ibid*.
[129] *Supra* note 12 at 188.

or individuals by gathering, storing, processing, diffusing, assessing and using data about humans so that potential or actual physical, ideological or structural violence can be directed against humans in order to influence their behaviour. This influence is brought about by coercive means and brings benefits to certain groups at the expense of others.[130]

Social Networking Sites like Facebook, Google, and many others are violating privacy of users through economic surveillance. Economic surveillance on corporate social media is surveillance of prosumers, who keeps on creating and sharing user-generated content, browse profiles and data, interact with others, join, create and build communities and co-create information. The corporate web platform operators and their third-party advertising clients continuously monitor and record personal data and online activities. They store, merge and analyse collected data. This allows them to create detailed user profiles and to know a lot about the users' personal interests and online behaviours. Social media that are based on targeted advertising sell prosumers as a commodity to advertising clients. There is an exchange of money for access to user data that allows economic user surveillance.[131]

Google also engages as Facebook in user surveillance for the end of capital accumulation. Google surveillance is primarily a form of economic surveillance. Google uses a powerful search algorithm. The details of the PageRank algorithm are secret. Basically small, automated programmes (web spiders) search the WWW, the algorithm analyzes all found pages, counts the number of links to each page, identifies keywords for each page, and ranks its importance. The PageRank algorithm is a form of surveillance that searches, assesses, and indexes the WWW.

### 2.7.4 PRIVACY BY DESIGN

Privacy by Design is an approach that promotes technology design and engineering to incorporate privacy into the design process from the start. The concept includes seven guiding principles on privacy and security. There are many facets to privacy by design, including software and systems engineering as well as administrative elements (e.g. legal, policy, procedural), other organizational controls, and operating contexts. "Privacy by design evolved from early efforts to express fair

[130] *Supra* note 12 at 189.
[131] *Supra* note 8 at 108.

information practice principles directly into the design and operation of information and communications technologies".[132]

One of the most important and developing practical areas of data protection is the concept of DPbD as referred to in the GDPR. Originally developed as a follow on from the data protection legal regime, it is now being recognized more widely, and is also being explicitly referred to and recognised in primary legislation itself. DPbD/PbD and data protection by default are important for organisations both in terms of being a legal obligation but also commercially in terms of being a competitive advantage.[133]

The concept of PbD is complementary to data protection law and regulation. The idea is acknowledged to have started with Dr Ann Cavokian, the Information and Privacy Commissioner for Ontario, Canada. She states that:

'the increasing complexity and interconnectedness of information technologies [requires] building privacy right into system design …the concept of Privacy by Design (PbD), …describe[s] the philosophy of embedding privacy proactively into technology itself – making it the default'.[134]

SNS companies are, by and large, private, for-profit corporations with a global reach and international profiles. They engage in actively shaping the debate on privacy on digital media through the ways in which they design the technologies of privacy on their sites and the options that they make available to users — the ways in which they revise and revisit these policies often causing strong reactions from users — and through their public discourses around privacy issues.

### 2.7.5 INTELLECTUAL PRIVACY IN THE DIGITAL AGE

American Scholar Neil Richards defines intellectual privacy as "it's is a zone of protection that guards our ability to make up our mind freely. More formally, intellectual privacy is the protection from surveillance or unwanted interference by others when we are engaged in the processes of generating ideas and forming beliefs –

[132] Ann Cavokian, Privacy by Design: Origins, Meaning, and Prospects for Assuring Privacy and Trust in the Information *available at*: https://www.researchgate.net/publication/289769458_Privacy_by_Design_Origins_Meaning_and_Prospects_for_Assuring_Privacy_and_Trust_in_the_Information_Era (last visited on May 30, 2022).
[133] Dr. Paul Lambert, *A User's Guide to Data Protection* 313 (Bloomsbury Professional, RH161BJ, 2016).
[134] www.privacybydesign.ca/about/ (last visited on May 30, 2022).

when we are thinking, reading, and speaking with confidants before our ideas are ready for public consumption".[135]

Richards argues that Intellectual Privacy, a special kind of privacy is necessary in a democracy because it allows us to develop our political beliefs free from the skewing effects of being watched, monitored, and judged.[136] Intellectual privacy secures the intellectual freedom to figure out what we believe about the world and our place in it. Intellectual privacy is essential to the development of our identities, but it is not the only kind of privacy that matters to our identities.

## 2.8 PRIVACY AND TERMS OF USE IN SOCIAL MEDIA

Every social media website has a privacy policy. Privacy policies explain how a website will use a visitor's personal information. These policies are perhaps most significant as tools by which the FTC can regulate unfair and deceptive trade practices.

In some of the most prominent court decisions addressing breach of contract claims arising from privacy policies, courts have not enforced the privacy policy against the website owner.

As applied to most commercial websites, the existing legislation requires that a privacy policy be posted and that the entity abide by that policy, but does not regulate the substance of that policy. No law prevents a website operator from sharing or selling personal information it has lawfully been given, although a website can be held liable for failing to notify its customers of its practice of selling or sharing such information. As long as they comply with the disclosure requirement, websites are free to state in their privacy policies that they will treat a visitor's personal information virtually any way they wish, arguably immunizing themselves from liability for such treatment.[137]

Thus, the true effect of privacy policies on an individual like a standard form of contact in general is dependent upon the drafter of the contract. A number of lawsuits have been filed by website users claiming breach of contract and promissory estoppel resulting from a website's violation of their privacy policy. However, applying a strict

[135] *Supra* note 111.
[136] Neil Richards, *Why Privacy Matters* 6-7 (Oxford University Press, New York, 2022).
[137] Daxton R. Stewart, (ed.) *Social Media and the Law A Guidebook for communications Students and Professionals* 56 (Routledge, New York, 2017).

standard form of contract analysis, a number of courts have denied any meaningful recovery for a website breaking promises it made in a privacy policy.[138]

## 2.9 CRITICISM OF PRIVACY

Etzioni stresses that it is a typical American liberal belief that strengthening privacy can cause harm. He stresses that privacy can undermine common goods (public safety, public health). Countries like Switzerland, Liechtenstein, Monaco, and Austria have a tradition of the relative anonymity of bank accounts and transactions. One sees money and private property as aspects of privacy about which the public should have no information. In Switzerland, the Federal Banking Act defines the bank secret. The Swiss Bankers' Association sees bank anonymity as a form of "financial privacy"[139] that needs to be protected and speaks of "privacy in relation to financial income and assets".[140] Most countries treat information about the income and profits of companies (except for public companies) as a secret, a form of financial privacy. The privacy-as-secrecy conception is typically part of the limited access concept of privacy.[141]

Control theories and limited access/control theories of privacy, in contrast, do not stress absolute secrecy of personal information as desirable, but rather highlight the importance of self-determination in keeping or sharing personal information and the different contexts in which keeping information to oneself or sharing it is considered important. In this vein, Helen Nissenbaum argues that the "right to privacy is neither a right to secrecy nor a right to control but a right to appropriate flow of personal information. In all of these versions of privacy theories, secrecy of information plays a certain role, although the exact role and desirability of secrecy is differently assessed.[142]

## 2.10 THE CONTRADICTIONS OF PRIVACY IN CAPITALISM: FACEBOOK AND GOOGLE

Social media corporations' managers often express the view that privacy is outdated. Google's Executive Chairman Eric Schmidt said for example: "if you have nothing that you do not want anyone to know, maybe you should not be doing it in the

[138] *Ibid.*
[139] Amitai Etzioni, *The limits of privacy 25* (Basic Books, New York, 1999).
[140] https://www.swissbanking.ch/en (last visited on May 30, 2022).
[141] *Supra* note 12 at 187.
[142] *Ibid.*

first place.[143] Facebook's co-founder and CEO Mark Zuckerberg said: "The goal of the company is to help people to share more in order to make the world more open and to help promote understanding between people."[144] Schmidt and Zuckerberg argue for massive data sharing on social media. They do not mention that this sharing is not primarily a sharing of data with friends and the public, but a sharing with Google and Facebook that are the largest data processors and data commodifiers in the world – which explains not just the recent rise of the term "big data", but also their interest in hiding their commercial interests ideologically behind the ideas of sharing and openness. Their claims are double-edged if one considers, for example, that Mark Zuckerberg in 2013 bought four estates that surround his house in Palo Alto's Crescent Park neighbourhood for US$30 million. He is concerned about his privacy. Zuckerberg's logic is as simplistic as it is mistaken: "Privacy is good only if you can pay for it, it is not good if it makes Facebook or Google obtain less profits."[145]

*Whereas social media corporations advocate openness, sharing of user data, and an end to privacy in order to maximize profits, they claim closure, secrecy, and financial privacy when it comes to their own global finance, profit, and tax issues. Social media is facing an economic antagonism between users' interest in data protection and corporate tax accountability on the one side and corporations' interest in user data's transparency/commodification and corporate secrecy on the other side*.[146]

## 2.11 EFFECTS OF THE RIGHT TO PRIVACY

Privacy as a basic human right touches upon fundamental needs and values associated with man's gregarious nature. Today, all democratic societies have come to realize that privacy is at the heart of all human rights. Certainly, the level of technological and economic development creates pressures to protect these privacy values through legal enforcement techniques. But even in the absence of such development, the value of and the basic human right to privacy may prevail irrespective of legal recognition. On the other hand, active claims for legal enforcement of the right seem to have a very direct relationship to the degree of threat

[143] *Ibid.*
[144] *Ibid.*
[145] *Id* at 188.
[146] *Ibid.*

posed to its survival. Certainly, this relationship holds at the level of legal development, and it supports the thesis that human rights such as privacy, although recognized by laws, are enforced only when the danger to underlying values is perceived. The values, themselves, may also be shared and implied in cultural norms, but often they are not articulated as legal norms until threatened.

The right to privacy is basic to every individual. Eclipse of privacy means eclipse of human dignity also. Justice Mathew rightly stated that "there can perhaps be no objection in regarding intrusion upon our privacy as a dignity tort. The harm caused by this intrusion is incapable of being repaired and the loss suffered in dignity is not susceptible of being made good of damages. The injuries to spiritual element in our otherwise mundane composition."[147] India has essentially been a gregarious society wherein cooperation and not competition, society and not solitude have been the dominant themes of its culture and civilization. Therefore, sometimes it is doubted whether privacy is a value of human relations in India. Certainly, it is wrong to suppose that the concept of privacy is alien to Indian culture. A man's house is his castle is a supreme and valid truth that is valued in all cultures and civilizations and India is no exception to it. The right to privacy in India had been recognized as a fundamental right of the citizen under Article 21 of the Indian Constitution in Puttaswamy case.

## 2.12 CONCLUSION

It may thus be summed up that the long search for a definition of 'privacy' has produced a continuing debate that is often sterile and ultimately futile for, in those legal systems recognize a common law right to privacy (or its equivalent), privacy is entrenched in the vocabulary of courts, where it is accorded statutory protection then privacy is simply what the legislature says it is. It is revealed that the entire description is predicated upon a civilized social life. Professor Westin has not deliberated over the role of privacy in the transformation of a natural society to a civilized one. It is abundantly clear from the foregoing study that the conceptual basis of privacy is an original sovereignty over oneself. Privacy is the recognition of individual autonomy and inviolate personality. It seeks protection of human dignity in a clear tune. Reputation and integrity of a person can be preserved out of the conceptual basis of privacy. It gives

147 Vide his Article, The Right to be Let Alone, 4 SCC Journal Section 3(1979).

place for genuine human emotions. It does not allow commercial exploitation of an individual's personality. Finally, it encircles a person's inner zone with a view to restore his status at art of his fellow member of society. Further, the contours of right to privacy remained undefined and an attempt has been made to analyze the scope, extent and effects of this right.

# CHAPTER-III

# PRIVACY POLICIES OF SOCIAL MEDIA

# CHAPTER III
# PRIVACY POLICIES OF SOCIAL MEDIA

## 3.1 INTRODUCTION

One of the great innovations of the 1990s and beyond is the sudden and rapid growth of social media, or social networking sites (SNS), which permit people to communicate quickly and easily through the Internet.[1]

SNS are discussed in the literature in a variety of ways. Ofcom, the UK's communication regulatory authority, defines SNS as:

*. . .sites, which allow users to set up online profiles or personal homepages, and develop an online social network. The profile page functions as the user's own webpage and includes profile information ranging from their date of birth, gender, religion, politics and hometown.*[2]

Different definitions of social media are found in the research literature. A few definitions of social media are as follows:

According to Albarran, social media represents "the technologies or applications that people use in developing and maintaining their social networking sites. This involves the posting of multimedia information (e.g., text, images, audio, video), location-based services (e.g., Foursquare), gaming (e.g., Farmville, Mafia Wars).[3]

In the words of Shirky, social media and social software are tools that "increase our ability to share, to co-operate, with one another, and to take collective action, all outside the framework of traditional institutions and organizations."[4]

According to Hunsinger and Senft, social media means "networked information services designed to support in-depth social interaction, community formation, collaborative opportunities and collaborative work."

According to Lovink, social media indicate a shift from HTML-based linking practices of the open web to liking and recommendation, which happen inside closed

[1] Stephen Currie, *How is the Internet eroding the privacy rights* 25 (Reference Point Press, United States, 2014).
[2] Ofcom, *Social Networking: A Quantitative and Qualitative Research Report into Attitudes, Behaviours and Use* (2008), *available at*: http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/report1.pdf (last visited on May 30, 2022).
[3] Christian Fuchs, *Social Media a critical introduction* 38 (Sage Publications India Pvt Ltd, New Delhi, 2017).
[4] *Id*. at 39.

systems. Web 2.0 has three distinguishing features: it is easy to use, it facilitates sociality, and it provides users with free publishing and production platforms that allow them to upload content in any form, be it pictures, videos, or text."[5]

Every social media website has a privacy policy. The purpose of a privacy policy is to outline how organizations will collect, maintain, and share user data. Often organizations write the privacy policy in a way that protects the organization more than the user.[6]

In this chapter, the researcher discusses different aspects of social media, privacy policy issues in domain of social media as well as different privacy policies of social media giants Facebook, Twitter and Google and their controversial features. With this discussion, the researcher analyses the nature of privacy policies of social media.

### 3.1.1 DEVELOPMENT OF SOCIAL MEDIA

The potential for computer networking to facilitate newly improved forms of computer-mediated social interaction was initially suggested during the infancy of the internet. Efforts to support social networks via computer-mediated communication were made in many early online services, including Usenet, ARPANET, LISTSERV, and bulletin board services. Many prototypical features of social networking sites (SNSs) were also present in online services such as America Online, Prodigy, CompuServe, ChatNet, and The WELL. Early social networking on the World Wide Web began in the form of generalized online communities such as Theglobe.com (1995), Geocities (1994), and Tripod.com (1995).[7]

The early communities focused on 'bringing people together' to interact with each other through chat rooms, and encouraged users to share personal information and ideas via personal web pages by providing easy-to-use publishing tools and free or inexpensive web space.

By the late 1990s, the nature of the sites began to change. User profiles became increasingly important as user demand for the ability to compile lists of connections, often referred to as 'friends', increased. The use of profiles with user data allowed users to search for and connect with other users with similar interests or shared connections.

[5] *Ibid.*
[6] A. W. Haynes, "Online privacy policies: Contracting away control over personal information" *Penn State Law Review* 111, 587 (2007).
[7] Laura Scaife, *Handbook of Social Media and the Law* 4 (Informa Law from Routledge, New York, 2015).

As user demand for such features increased, sites developed increasingly sophisticated offerings that allowed users to find and manage friends. In 1997, the 'next generation' social networking sites began to flourish with the introduction of sites such as SixDegrees.com.[8]

The third generation of networking sites began in the early 2000s. Makeoutclub was introduced in 2000, with Hub Culture and Friendster following in 2002. Facebook was first introduced (in 2004) as a Harvard social networking site.

Such sites soon became part of users' internet consumption, and by 2005, it was reported that MySpace was getting more page views than Google. Facebook became the largest social networking site in the world in early 2009.

### 3.1.2 SOCIAL MEDIA AND SOCIAL NETWORK

Owing to the explosion of Web 2.0 and the increasing sophistication of technologies that can be used to access web content, users both produce and consume significant quantities of multimedia content. Moreover, this behaviour when combined with social networking (i.e. communication between users through online communities) has formed a new internet era where multimedia content sharing through social networking sites is an everyday practice.[9]

A social networking service is a platform to build social networks or social relations among people who, for example, share interests, activities, backgrounds or real-life' connections. A social network service consists of a representation of each user (often a profile), his or her social links, and a variety of additional services. Most social network services are web-based and provide means for users to interact over the internet, such as email and messaging. The service usually allows individuals to create a public profile, to create a list of users with whom to share connection, and view and cross the connections within the system.[10] In recent years, social networking sites have become increasingly varied and they now commonly incorporate new information and communication tools, such as mobile connectivity, photo/video/sharing, and blogging. Online community services are sometimes considered to be social networking sites, though in a broader sense, social networking site usually means an individual-centred

[8] *Ibid.*
[9] http://www.alexa.com (last visited on May 30, 2022).
[10] D.M. Boyd and N.B. Ellison "Social network sites: definition, history and scholarship" 13(1) *Journal of Computer-Mediated Communication* 210-230 (2007).

service, whereas online community services are group-centred. Social networking sites allow users to share ideas, pictures, posts, activities, events, and interests with people in their network.

### 3.1.3 NATURE OF INFORMATION SHARING

When a communication is sent via a social networking site, be it via a Smartphone, tablet or web browser, the content is normally only saved on the social networking site server. This type of cloud computing is a common way in which the majority of social networking sites operate.[11]

Although different hardware may be used to access the site, the way in which the social networking site server stores the information is the same. The use of the site will involve the storage of a number of pieces of data about a user, such as the user's IP address (location, etc.). If a user accesses their account from a different computer or device, then this will also be recorded and assigned to that user. In this way, the activity logs of that user and their movement can be recorded such as their communications and their geographic migration.

### 3.1.4 TYPES OF DATA PROCESSED

Several types of data may be shared via social networking sites. Table 3.1 shows the types of data that may be uploaded via a social networking site and the groups of users with which other users may wish to share their data.[12]

[11] Laura Scaife, *Handbook of Social Media and the Law* 6 (Informa Law from Routledge, New York, 2015).
[12] *Id.* At 7.

**Table: 3.1 Taxonomy of social networking data**

| | |
|---|---|
| **Service Data** | Data a user may provide to a social networking site in order to set up an account. Such data might include a user's legal name, age, home address, gender, and email address. |
| **Disclosed Data** | Data which the user posts on their own page, e.g. status updates, tweets, blog entries, photographs, messages, comments, and so on. |
| **Entrusted Data** | Data posted on other account holders' pages, often similar in content to disclosed data, expect that the user relinquishes a degree of control over the data once it has been posted. Although such data may be deleted, the replication or re-sharing of the data, who views it, or the comments which are posted next to it may not be so easy to control. |
| **Incidental Data** | Data posted by other users, e.g. comments, photographs taken by others that a user is tagged in. The user does not control this data and it is not created by the user who is the subject matter of the posting |
| **Behavioral Data** | Data collected by the social networking site which concerns a user's habits and preferences. The data is gathered by recording user activity and interactions with other users. It might include games played, topics the user writes about, news articles accessed, etc. |
| **Derived data** | Data about a user that is derived from all other sources of data. |

### 3.1.5 CATEGORIES OF SOCIAL MEDIA

Social media sites, applications, and services fall into one or more of several fundamental categories. Because of constantly evolving technology and the growing mainstream use of social media, certain websites, web services, and applications fit into more than one category and may evolve over time to fall into different categories.

### 3.1.6 TYPES OF SITES

Social Networking sites (SNSs) are put into different categories. A few of them are as follows:

| | |
|---|---|
| **Blog** | A 'web log' or website listing posted information and other content dated in reverse chronological order, self-published by authors (known as bloggers) on sites such as Blogspot, WordPress, Tumblr and Blogger. |
| **Social and Business networking site** | A website where individual, corporate, and organizational users can connect to other users and display online their networks of friends and contacts for other users to see and form connections with. Prominent examples include Facebook and Linkedln. |
| **Digital Media sharing site** | A website where users can upload and share videos, photos, and accompanying text. YouTube and Flickr are the main sites in this category. |
| **MMPORG site** | MMPORG (Massively multiplayer Online Role-Playing Game) site is a genre of video games that can be played by several users simultaneously regardless of physical location, over the Internet. Players adopt avatars to represent themselves in the virtual world online and interact with each other. SecondLife is the most popular example of this category. An avatar is a customized character in digital form created by an online user to personify his presence on a website and interact with other users, such as in online gaming communities, virtual worlds or forums. |
| **Virtual World** | A computer-based environment, such as a MMORPG, created to simulate a real or fictitious environment, often containing elements of both. Users of online virtual worlds interact through their avatars. Popular examples include ActiveWorlds, Kaneva, and SecondLife. |

### 3.1.7 SOME POPULAR SOCIAL MEDIA PLATFORMS

**FACEBOOK -** Facebook operates as a social networking site based on interconnection with other users to generate content. Users must register before using the site, after which they may create a personal profile, add other users as friends, and

exchange messages, including automatic notifications when they update their profile. Additionally, users may join common-interest user groups, organized by workplace, school or college, or other characteristics.

**Instagram -** A photo-sharing service where users can share photos that have had digital filters added to them onto social networks like Facebook or Twitter. The site is owned by Facebook. Instagram has become an increasingly popular social network that is focused on image sharing. Its acquisition allowed Facebook to strengthen its presence in the realm of content-sharing networks.

**WhatsApp –** WhatsApp is mobile phone instant messaging app which was acquired by Facebook in 2014, now its web edition is also available. WhatsApp and Instagram are examples of social media that competed with Facebook, which meant that Facebook became horizontally integrated in social media after acquiring the companies.

**Google+ -** A social network launched by Google in 2011 where members can connect with friends and other people in their 'circle' and see what other people are posting through their 'stream'. Members can also 'hang out' and video chat.

**YouTube -** An online video community that allows users to publicly post, share, and view original videos, with a forum for user comments and a platform for creating individual channels. YouTube provides for video embedding, allowing users to link videos posted on YouTube to their profiles on Facebook. Many businesses also send samples of their products to respected bloggers, e.g. in fashion and beauty to review or promote their products.

**Twitter -** Twitter is the micro-blogging site that was created by Jack Dorsey in March 2006. Twitter allowed its users to send and read text-based posts of up to 140 characters, known as "tweets" in real-time, which gained worldwide popularity with over 300 million users as of 2011. It was described as the "SMS" of the Internet.

**LinkedIn -** A professional networking website where members can maintain connections with other members, establish connections to contacts of members in their network, and be introduced to other members for help in job searches and other career-related goals.

**WordPress -** An open-source software program that allows users to publish websites or blogs. WordPress was originally created as al blog publishing system but later on it has evolved to support other web content types including more

traditional mailing lists and forums, media galleries, membership sites, learning management systems and online stores.

**Friendster -** Originally a social networking site that was re-launched in 2011 as a social gaming site. Also has a micropayments component called Friendster Wallet, enabling pre-paid payments between members on their sites for virtual gifts and games.

**Pinterest -** A pin-board style social sharing site where users can create and manage image collections based on themes such as events, interests, and hobbies. Users can 're-pin' other people's images to their own board, like images or search through categories that interest them.

**Delicious (formerly del.icio.us) -** A social bookmarking site where members can save their website bookmarks in a central online location for future retrieval from any Internet browser at any time, and share those bookmarks with friends.

**Flickr -** An online photo management and sharing application that enables members to make the photo and video content they upload available on the web for viewing and commenting (public and private). Flickr is for personal (non-commercial) use only.

More than 200 social networking sites of worldwide impact are known today and this number is growing fast. Many of the existing top websites are either pure social networking sites or offer some social networking capabilities.[13]

## 3.2 PRIVACY POLICY ISSUES OF SOCIAL MEDIA

The term "privacy policy" implies that the organization is going to protect or keep user data private when in fact privacy policies explain how the organization will collect, maintain, store, and share data.

Social media and social networking sites (SNS) have risen sharply in popularity and widespread use, allowing new forms of socialization, sharing, and communication between people. This new state of communication raises new privacy questions. The sheer numbers of users and the fact that their communication is very public are new factors, unknown at the time of Warren and Brandies.

The main point about SNS is that they are popular with millions of users worldwide and they promote a self-exhibiting, self-disclosing culture. In that respect, a great deal of personal information becomes public or semi-public without the users

[13] http://www.alexa.com (last visited on May 30, 2022).

entirely understanding the ramifications for their privacy.[14] Given the fact that most users are young people, this means that new conditions and understandings of privacy as imposed or initiated by SNS will become established as the new norm very quickly. It is therefore, important to understand what loss of privacy incurred in the context of SNS. Here, the researcher discusses some of the basic problematic issues connected with privacy policies of social media.

### 3.2.1 AMBIGUITY IN LANGUAGE OF PRIVACY POLICY

Privacy policies are difficult to understand and contain ambiguous language that leaves out relevant information or contain words that leave statements made in the privacy policy open to interpretation.[15] Furthermore, privacy policies tend to be long boring documents with ambiguous and misleading language. Reidenberg and others[16] opined, "Without clear affirmative statements, privacy policies are, in effect meaningless. They provide no true indication to users of the website's actual practices, and they provide declarations that would be unenforceable".

Multiple studies in privacy policy readability found that although privacy policies are the only means for an organization to communicate data sharing and collection policies, the ambiguous, vague, and confusing language used undermines the effectiveness and purpose of the privacy policy.[17] Furthermore, Waldman argued that organizations do not write privacy policies with the average user in mind. Rather privacy policies are written in adherence to laws and government guidelines that focus on giving notice to users but not effectively communicating the organization's procedures.[18]

### 3.2.2 WEB TRACKING

Privacy policies do not disclose all third-parties who may access and collect user data. Web pages are not static and may contain "content" from a third-party unknown to the user.[19] In a 2018 study, Libert discussed that the content on a website allows third

[14] Friendster was the first SNS launched in 2002, with MySpace and Linkedln following in 2003, Facebook in 2004 and Twitter in 2006.
[15] Julie J. Beyer, *Privacy: The endangered species of the digital era* 81 (Faculty of Utica College, ProQuest LLC, 2018).
[16] *Id.* at 2.
[17] *Id.* at 22.
[18] *Ibid.*
[19] *Id.* at 3.

parties to engage in a practice called web tracking, which allows third parties to collect data on user browsing habits and preferences.

Facebook states that it collects information from partners. Different Advertisers, app developers and publishers share information with Facebook with the help of different tools, including social plug-ins (such as the Like button), Facebook Login. These partners provide information about users' activities off of our Products – including information about users device, websites users visit, purchases users make, the ads users see and how users use their services – whether or not users have an account or are logged in to Facebook Products.[20] It implies that different advertisers, app developers and publishers using Facebook's services keep on tracking users' activities online as well as offline and share users' information with the Facebook. Similarly, Twitter and Google allow third partners to use their API and third partners keep on tracking users' activities online and offline, hence share users' information with Twitter and Google.[21]

### 3.2.3 NOT READING PRIVACY POLICY BY USERS

Another issue with privacy policies is that most users do not read them. Research shows that users have concerns for how data is collected and stored, yet most users ignore the most important tool available in data protection, which is to read and understand the organization's privacy policies.[22]

Although young people claim, or appear to be, both concerned about and aware of privacy issues, they usually do not take any precautionary measures to protect themselves.[23]

### 3.2.4 TARGETED ADVERTISING

Social Networking Sites like Facebook, Google and many others are violating privacy of users through economic surveillance. Economic surveillance on corporate social media is surveillance of prosumers, who keeps on creating and sharing user-generated content, browse profiles and data, interact with others, join, create and build

[20] Facebook Privacy, *available at:* https://www.facebook.com/privacy/explanation/ (last visited on May 30, 2022).
[21] https://twitter.com/en/privacy https://policies.google.com/privacy?hl=en-IN&fg=1 (last visited on May 30, 2022).
[22] *Supra* note 15 at 3.
[23] Monroe E. Price, Stefaan G. Verhulst, *et.al.* (eds.), *Routledge Handbook of Media Law* 476 (Routledge, New York, 2013).

communities and co-create information. The corporate web platform operators and their third-party advertising clients continuously monitor and record personal data and online activities. They store, merge and analyse collected data. This allows them to create detailed user profiles and to know a lot about the users' personal interests and online behaviours. Social media that are based on targeted advertising sell prosumers as a commodity to advertising clients. There is an exchange of money for the access to user data that allows economic user surveillance.

Google also engages as Facebook in user surveillance for the end of capital accumulation. Google surveillance is primarily a form of economic surveillance. Google uses a powerful search algorithm. The details of the PageRank algorithm are secret. Basically small, automated programmes (web spiders) search the WWW, the algorithm analyses all found pages, counts the number of links to each page, identifies keywords for each page, and ranks its importance. The PageRank algorithm is a form of surveillance that searches, assesses and indexes the WWW.[24]

The use of targeted advertising and economic surveillance is legally guaranteed by Facebook's privacy policy. Facebook can largely regulate itself in what it wants to do with user data because it is a company that is legally registered in Palo Alto, California, U.S.A. Facebook's data policy is a typical expression of a self-regulatory privacy regime, in which businesses largely define themselves by how they process personal user data. The general perception in privacy and surveillance studies is that there is very little privacy protection in the United States, and that the United States lags behind Europe in protecting privacy. Also, US data protection laws only cover government databanks and, due to business considerations, leave commercial surveillance[25] untouched in order to maximize profitability.[26]

### 3.2.5 SELF-REGULATION

Facebook's terms of use and its data policy are characteristic of liberal US data protection policies that are strongly based on business self-regulation. They also stand for the problems associated with a business-friendly self-regulatory privacy regime – if privacy regulation is voluntary, the number of organizations engaging in it tends to be very small: "Self-regulation will always suffer from the perception that it is more

[24] *Supra* note 2 at 195.
[25] *Ibid.*
[26] *Id.* at 196.

symbolic than real because those who are responsible for implementation are those who have a vested interest in the processing of personal data." In the United States, we call government interference domination, and we call marketplace governance freedom. We should recognize that the marketplace does not automatically ensure diversity, but that (as in the example of the United States) the marketplace can also act as a serious constrain to freedom".[27]

### 3.2.6 USERS' PERCEPTION OF PRIVACY POLICIES

A privacy policy is supposed to communicate to a user how an organization collects, stores, and shares data so that the user can decide whether to utilize the organization's online services. However, when an organization does not notify users about who is collecting the data, the user is unable to form an opinion on the safety and security of the organization's website.

Since the 1960's, researchers have been studying privacy in an era of technological advances. When e-commerce became prevalent in the mid-1990s, researchers began conducting studies about users' perceptions of privacy policies. A study conducted by Fogg[28] et al. and commissioned by Consumer WebWatch examined how users determine whether a website is credible and what users notice when they visit websites. Results of this study showed that users focus more on design elements of a website and, unless specifically asked, do not consider privacy policies when determining website credibility.

Further studies on Prominence-Interpretation theory opined there are two things users take into consideration when visiting a website; a user will notice elements on the page and then form judgments about the website.[29] Fogg indicated that if users do not notice an organization's privacy policy, then users would not consider if a website were credible because it has a privacy policy.

Most users are unaware of an organization's privacy protection practice because users do not read privacy policies. A study conducted by Obar and Oeldorf-Hirsch[30] found that most users skip reading privacy policies by clicking on the "I agree to the terms…" checkbox that pops up when starting an account with a new service. The

[27] *Supra* note 2 at 196
[28] *Supra* note 15 at 80.
[29] *Id.* at 21.
[30] *Id.* at 4.

excuses given by users in the study ranged from joining the service because friends and family are using the service or that the user is too lazy to read the policy. Obar and Oeldorf-Hirsch[31] concluded that the current framework of notice and choice are not effective and cannot protect user privacy if the user does not read the privacy policy.

### 3.2.7 STANDARD FORM OF CONTACT IN SOCIAL MEDIA PLATFORM

The primary function of the Internet is to connect people. These connections can create a privity of contract between websites and users. Contracts between websites and users are typically seen in the form of term of use. These agreements are adjudicated under standard form of contract doctrine because they are perceived as non-negotiable.

The traditional rule holds that in order for a contract to be valid the parties must reach a "meeting of the minds." In other words, both parties to the contract must agree to be bound by mutually understood terms. In recent years, some critics have asserted that the traditional rules of contract law "based on the ideal of two humans meeting in person to agree to terms, have been modified almost to the point of non-existence." These critics cite the fact that courts do not consider the actual state of mind of the parties, but rather what they objectively conveyed to each other when forming the contract – known as "objective theory of contract".[32]

Online contracts have traditionally been categorized as "browse-wrap" or "clickwrap" agreements, although that distinction can be blurred at times. Regarding browse-wrap agreement, courts "have held that 'the validity of a browse-wrap turns on whether a website user has actual or constructive knowledge of a site's terms and conditions prior to using the site." Thus, in order to be bound, parties need not have "meeting of the mind." Rather, a "reasonable communication" of terms will suffice.[33]

Thus, standard-form contract doctrine on the web, have great significance for user privacy. In some of the most prominent court decisions addressing breach of contact claims arising from privacy policies, courts have not enforced the privacy policy against the website owner. As applied to most commercial websites, the existing legislation requires that a privacy policy be posted, and that the entity abide by that policy, but does not regulate the substance of that policy. No law prevents a website operator from

[31] *Supra* note 15 at 22.
[32] Daxton R. Stewart, *Social Media and the Law A Guidebook for Communication Students and Professionals* 56 (Routledge, New York, 2013).
[33] *Ibid.*

sharing or selling personal information it has lawfully has been given, although a website can be held liable for failing to notify its customers of its practice of selling or sharing such information. As long as they comply with the disclosure requirement, websites are free to state in their privacy policies that they will treat a visitor's personal information virtually any way they wish, arguably immunizing themselves from liability for such treatment.

Thus, the true effect of privacy policies on an individual like standard form of contacts in general, is dependent upon the drafter of the contract. A number of lawsuits have been filed by website users claiming breach of contract and promissory estoppel resulting from a website's violation of their privacy policy. However, applying a strict standard form contract analysis, a number of courts have denied any meaningful recovery for a website breaking promise it made in a privacy policy.[34]

## 3.3 FACEBOOK'S PRIVACY POLICY AND ITS SOME CONTROVERSIAL FEATURES

Facebook is the most popular social networking site (SNS). SNSs are web-based platforms that integrate different media, information and communication technologies that allow at least the generation of profiles that display information describing the users, the display of connections (connection list), the establishment of connections between users displayed on their connection lists, and communication between users.[35]

Facebook was created in 2004 by Harvard University student Mark Zuckerberg. It was based on the concept of the university's "facebook" — a directory of student names with a picture, typically organized by graduating class year. In its first iteration, Facebook was a program called Facemash, which Zuckerberg developed, that allowed Harvard students to rank photographs of their classmates according to attractiveness. Zuckerberg obtained the photographs by hacking into Harvard's database of student identification images. Harvard University administration shut down the site a few days after Zuckerberg began disseminating it. However, a few months later Zuckerberg began development of the thefacebook.com. Thefacebook.com was launched in February 2004 and only allowed Harvard University students to join. In March of 2004, thefacebook.com expanded to Columbia University, Stanford University, and Yale

[34] *Supra* note 32 at 59.
[35] *Supra* note 2 at 183.

University. At this time Eduardo Saverin, Dustin Moskovitz, Andrew McCollum, and Chris Hughes joined Zuckerberg in the development and management of the website. Very quickly, thefacebook.com expanded to include Ivy League universities and Boston area colleges. It continued to expand and by 2006 Facebook was available to anyone over the age of 13. By 2012, Facebook announced it had reached its one-billionth user. Facebook is now a publicly-traded company that has a net worth in the billions of dollars. Its primary source of revenue is through advertising, with a small amount of additional revenue coming from fees and payments for virtual services, such as games.[36]

Facebook wants to assure users that it deals responsibly with their data and those users are in full control of privacy controls. Therefore, as an introduction to the privacy issue, it wrote: "We give you the power to share as part of our mission to make the world more open and connected."[37] Facebook uses targeted advertising in which it sells user data to advertisers: "We want our advertising to be as relevant and interesting as the other information you find on our Services. With this in mind, we use all of the information we have about you to show you relevant ads."[38]

In its privacy policy, Facebook avoids speaking of selling user-generated data, demographic data and user behaviour. It instead uses the phrase "sharing information" with third parties ("third parties we can share information with about you"), which is a euphemism for the commodification of user data. The word sharing/share appear 36 times in[39] Facebook's data policy from January 2015, the terms sell/selling/sale/commodity not a single time.[40]

There are no privacy settings on Facebook that allow users to disable advertisers' access to their data (there are only minor privacy settings relating to "social advertising" in Facebook friend communities). Facebook does not ask users whether they find targeted advertising necessary and agree to it.[41]

Facebook in general uses targeted advertising. There is an opt-out in the advertising preference option for Facebook's use of data from across the web (e.g.

[36] JD Christopher T. Anglim (ed.), *Privacy Rights in the Digital Age* 188 (Grey House Publishing, USA, 2015).
[37] www.facebook.com (last visited on May 30, 2022).
[38] *Supra* note 2 at 196.
[39] *Ibid.*
[40] *Supra* note 2 at 197.
[41] *Ibid*.

which websites a user visits and which apps s/he uses on her/mobile phone). Even if one opt-out of this option, Facebook continues to target ads based on the user's Facebook behaviour and profile data and continues to present the same amount of ads.[42]

"If you turn off online internet-based adverts you'll still see the same number of adverts, but they may be less relevant to you."[43] Facebook assumes that its targeted algorithm can calculate and predict interests and tastes. Its strategy excludes that some users may not at all want to have their data monitored, analysed and commodified.[44]

Users must agree to the privacy terms in order to be able to use Facebook and thereby they agree to the use of their self-descriptions, uploaded data and transaction data to be sold to advertising clients. Given the fact that Facebook is the second most used web platform in the world, it is unlikely that many users refuse to use Facebook because doing so will make important new contacts, and may result in being treated as outsiders in their communities. Facebook coerces users into agreeing to the use of their personal data and collected user behaviour data for economic purposes.[45]

If you do not agree to the privacy terms that make targeted advertising possible, you are unable to use the platform. Users are not really asked if their data can be sold to advertisers, therefore one cannot speak of user consent. Facebook utilizes the notion of "user consent" in its privacy policy in order to mask the commodification of user data as consensual. It bases its assumption on a control theory of privacy and assumes that users want to sacrifice consumer privacy in order to be able to user Facebook.[46]

The structure and function of Facebook work powerfully in the service of motivation. If you want to summon people to a cause, solicit donations, urge people to vote for a candidate, or sell a product, few media technologies would serve you better than Facebook does. Facebook is great for motivation. It is terrible for deliberation.[47]

The impact on the privacy of individuals using Facebook has been an issue from its initial iteration as Facemash. When the Harvard University administration shut it down one of the reasons, they gave was the privacy concern of disseminating students' pictures without their consent. This concern has persisted, despite Facebook's

[42] *Ibid.*
[43] www.facebook.com (last visited on May 30, 2022).
[44] *Supra* note 2 at 197.
[45] *Ibid*.
[46] *Ibid*.
[47] Siva Vaidhyanathan, *Antisocial Media, How Facebook Disconnects Us and Undermines Democracy* 7 (Oxford University Press, New York, 2018).

continued effort to assure its users that the information they generate by using Facebook is adequately protected.[48]

Facebook by its very nature, raises fundamental privacy challenges because it enables users to disclose unprecedented volumes of highly personal information, not only to friends and friends of friends, but, depending on one's privacy settings, to very large and unfamiliar audiences as well. The researcher discussed some major controversial Facebook features: News Feed, Beacon, Facebook Apps, and Photo Sharing.

### 3.3.1 NEWS FEED

Facebook's first major privacy incident occurred in 2006 with the launch of News Feed, a new feature that created a stream of headlines sent to all users based on the activities of their friends throughout the day including newly uploaded pictures, changes in relationships, and so on. News Feed automatically enrolled all Facebook users on an opt-out basis and the feature lacked any controls over what information was shared or with which friends. Users reacted with alarm over the unintended consequences of Facebook broadcasting their activities to their entire list of friends. Within days, Facebook CEO Mark Zuckerberg released an open letter apologizing to users for "[messing] this one up" by failing to build in privacy controls from the outset, which Facebook promptly corrected by introducing new controls.[49]

### 3.3.2 BECON

A year later, Facebook released Beacon, an addition to their developing ad platform. Beacon provided targeted ads based on items a user purchased or browsed on the websites of some forty-four partner sites and shared this information with a user's friends via the News Feed. Although early versions of Beacon apparently included a global opt-out capability, Facebook removed this feature prior to release in favour of more limited privacy controls. Moreover, even if a Facebook user decided not to share such information with a friend, Facebook still received it. Although commentators quickly labelled Beacon "a privacy disaster waiting to happen," Facebook decided to ride out the controversy, hoping that consumers might still "fall in love" with Beacon

[48] *Supra* note 36 at 188.
[49] Ira S. Rubinstein and Nathaniel Good, "Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents" 28 (2) *Berkeley Technology Law Journal* 1393 (2013). DOI: https://www.jstor.org/stable/24119897

once they understood it better. Instead, Facebook users revolted, voicing concerns over the risk of embarrassment or the ruining of a surprise if an activity at a partner website was shared with the wrong friend or at the wrong time. As the controversy heated up, Facebook tweaked Beacon's privacy notice and eventually converted Beacon to an opt-in model, with a global opt-out feature that turned it off entirely. But the damage was already done: Facebook discontinued Beacon in 2009 but not before settling a class action lawsuit for $9.5 million.[50]

### 3.3.3 FACEBOOK APPS

In 2007, Facebook launched the Facebook Platform, a set of Application programming interfaces ("APIs") and tools enabling developer to create hundreds of thousands of third-party applications ("apps") for Facebook users. Popular apps include games, instant messaging, and a forum for social activists to share their ideas. Once approved by Facebook, apps may retrieve or post information to member profiles and request information about users and their friends. Users are required to grant access privileges to apps as a condition of installing them. However, most applications were given access to far more private information than they needed. Moreover, many users lacked understanding of what data they were sharing when they installed an app, either because they hurried through the installation process and ignored notices or relied on the fact that applications ran within the boundary of Facebook, wrongly inferring that their data would remain within the Facebook network. These issues led Canadian privacy regulators to investigate such complaints. They found that Facebook lacked adequate safeguards effectively restricting outside developers from accessing a user's profile information,[51] and called for technological measures restricting access to the information that was actually required to run a specific application.

### 3.3.4 PHOTO SHARING

Facebook allows users to share photos with their friends in multiple ways. Users can upload photos to an album, post photos directly to their profile, or post directly to someone else's profile. Once a photo has been posted, users may tag it, which creates a link between the tagged photo and a person, page, or place, thereby revealing additional information about the identity and associations of the people depicted in the

[50] *Id.* at 1394.
[51] *Id.* at 1395.

photo. Users may tag themselves or their friends, who will be notified of the tag. Tagging people also alters the potential audience who can view a photo. Users can remove the tag from the photo, which removes the explicit reference to the user (by eliminating the link to the user's profile), but the photo remains on Facebook, accessible from any friends' profiles to which it is cross-linked.

As Facebook tagging has taken off, so has the desire of individuals to retain control over unflattering images. Individuals are especially concerned about the unintended results of tagged photos, which may cause embarrassment or humiliation if family, employers, school officials, or law enforcement officials see photos meant for different eyes. These tagging three distinct individuals — the photographer, the tagger, and the tagged subject — who may disagree over the propriety of tagging a given photo. These issues will likely become even more prevalent given Facebook's creation of the Photo Tag Suggest feature, which uses facial recognition technology to help users tag even more photos. Users can opt out of this feature and provide direct feedback about any items that friends post or share.

After the rollout of Photo Tag Suggest, Facebook announced changes in August 2011 to enhance users' control over who could see photos, tags, and other content. The main change was moving the privacy controls from a settings page to an inline control adjacent to the affected photos. Each photo or album now has a drop down menu that allows a user to control exactly who can access it. Facebook also added a new Profile Tag Review feature that allowed users to approve or reject any photo in which they were tagged before it became visible on their profile. Finally, Facebook changed the way the options for removing tags or content on Facebook are presented to users. They now have options to remove a photo from their profile, remove the tag itself, send a message to the owner or tagger, or request that the content be taken down. The Irish regulators raised some initial concerns about photo tagging but were generally satisfied by these new controls.

Photo Sharing introduces a new set of issues involving two kinds of peer-produced privacy violations. The first arises due to the "shrinking perceived audience" problem, in which users indiscriminately disclose potentially embarrassing photos because they forget just how many people can view them notwithstanding their intentions to share them with a much smaller audience. The second implicates the social fallout from tagging disputes, where the photographer, the tagger, and the subject

disagree over whether the photo should be untagged, made private, or even removed. As Grimmelmann notes, Facebook is the catalyst of these privacy violations, not the perpetrator.[52]

### 3.3.5 FACIAL RECOGNITION TECHNOLOGY (FRT)

A biometric technology that identifies people by measuring and analyzing their physiological or behavioural characteristics. Biometric technologies were developed to identify people through characteristics such as their faces, fingerprints, hands, eye retinas and irises, voice, and gait. Unlike conventional identification methods, including a card to gain access to a space or a password to log on to a computer system, biometric technologies determine characteristics that are unique to each person and would be difficult to alter. There has been strong opposition to the commercial use of facial recognition. Google removed facial recognition apps and services. Europe ordered Facebook to discontinue the use of facial recognition for photo tagging.[53]

An FRT system has four basic parts: a camera to capture an image, an algorithm to create a faceprint (also known as a facial template), a database of stored images, and an algorithm to compare the captured image to the database of images or a single image in the database.[54]

FRTs are able to perform several functions, including (1) detecting a face in an image; (2) estimating personal characteristics, such as an individual's age, race, or gender; (3) verifying identity by accepting or denying the identity claimed by a person; and (4) identifying an individual by matching an image of an unknown person to a gallery of known people. FRT systems can generate two types of errors — false positives (reporting an incorrect match) or false negatives (not reporting a match when one exists). Studies of FRT algorithms have indicated that this technology has improved over time. Error rates continue to decline, and algorithms are getting better at identifying individuals from images of poor quality or that are captured under low light. Also, certain controlled tests have indicated that facial recognition algorithms surpassed humans in accurately identifying whether pairs of face images, taken under different lighting, were images of the same person or different people.[55]

[52] *Supra* note 47 at 1398.
[53] *Supra* note 36 at 190.
[54] *Ibid.*
[55] *Ibid.*

Individuals continue to upload billions of pictures to social networking and other Internet sites, which develop a large repository of facial images. These images in turn are often linked to names or other personal information. The combination of these two trends may make it feasible to soon identify almost any individual in several public spaces. Privacy organizations, who have expressed concerns about the commercial application of facial recognition technology, have generally focused on (1) how it affects the ability of individuals to remain relatively anonymous in public; (2) the capacity to track individuals across locations; and (3) use of facial recognition without the individuals' knowledge or consent.[56]

Several government, industry, and privacy organizations have proposed or are developing privacy guidelines governing the commercial use of FRT, including describing how commercial organizations collect, use, and store data.[57]

Many, including privacy groups and government agencies, have asserted several privacy concerns on the commercial use of FRT. They claim that, if FRT use became widespread, it could allow businesses or individuals to identify almost everyone in public without their knowledge or consent and to monitor the locations, movements, and associates of individuals. They have also expressed concerns that information collected or associated with FRT could be used, shared, or sold in ways that consumers do not understand, anticipate, or want to consent to.[58]

Industries using FRT have generally agreed that a code of conduct should be implemented that would require companies using facial recognition to be transparent about their use of the technology. A notice or a sign might be the answer, but how much information would be required and through what means to gain consent of those being surveilled by FRT remain a hotly disputed issue.[59]

## 3.4 Twitter

A blog is a website that features periodically published postings that are organized in reverse chronological order so that the newest postings are shown first. A microblog is a further development of the blog concept: one shares short messages with the public and each user has a contact list of persons who are following these messages.

[56] *Ibid.*
[57] *Id. at 191.*
[58] *Ibid.*
[59] *Id.* at 191.

Microblogging is like sending SMS online to a large number of people. A microblog is "an Internet-based service in which: (1) users have a public profile where they broadcast short public messages/updates (2) messages become publicly aggregated together across users; and (3) users can decide whose messages they wish to receive, but not necessarily who can receive their messages". The two most popular microblogs in the world are Twitter and Weibo. The Chinese company SINA owns Weibo, which was created in 2009. Twitter was created in 2006. It is owned by Twitter Inc., a company founded by Jack Dorsey that is based in San Francisco.[60]

Twitter enables users to communicate with large numbers of interested people, known as followers, by sending out short messages — known as tweets—about their activities, thoughts, and experiences.[61]

### 3.4.1 CAPITAL ACCUMULATION ON TWITTER

Twitter started as a profit-oriented corporation without a business model. At first it did not use advertising. In September 2009, it revised its terms of use, so that advertising and targeted advertising became possible. But advertising was not used. In April 2010, Twitter announced that advertising would be introduced in the near future. Twitter's terms of use significantly grew in length and complexity, and set out the company's ownership rights with respect to user-generated content. In 2011, Twitter's business model that is based on targeted advertising came into full effect.[62]

Twitter's capital accumulation model uses three mechanisms: *promoted tweets, promoted trends, promoted accounts.* Promoted tweets are advertising tweets that appear at the top of search result lists for searches conducted by specifically targeted user groups. "Use Promoted Trends to drive conversations and interest around your brand or product by capturing a user's attention on Twitter". "The Promoted Account is featured in search results and within the Who To Follow section. Who To Follow is Twitter's account recommendation engine and identifies similar accounts and followers to help users discover new businesses, content, and people on Twitter."[63]

When one searches on Twitter for content or a hashtag, current tweets, people results/accounts and worldwide Twitter trends are displayed. Twitter's advertising

[60] *Supra* note 2 at 179.
[61] *Supra* note 1 at 72.
[62] *Supra* note 2 at 207.
[63] *Supra* note 2 at 242.

strategy manipulates the selection of Twitter search results, displayed accounts and trends. Not those tweets, accounts and trends that attain most attention are displayed, but preference is given to tweets, accounts and trends defined by Twitter's advertising clients. Twitter advances a class-structured attention economy that privileges economically powerful actors over everyday users. If you are a large company with a huge advertising budget, then it is easy for you to buy attention on Twitter. If you are an everyday user without an advertising budget and without much time, you will, in contrast, have a much harder time promoting your tweets and your accounts as trend on Twitter.[64]

### 3.4.2 TWITTER'S TERMS OF SERVICE

As is true of most online services, however, privacy and the use of data are a concern. Twitter's own website and privacy policy states: "When using any of our Services you consent to the collection, transfer, storage, disclosure, and use of your information as described in this Privacy Policy." Also, most are aware that what you Tweet is for public view. There is an option to make your account private and to choose who sees your Tweets, but your account name is still visible to the public.[65]

Other serious privacy issues exist. For example, Twitter collects data from you when you Tweet, but it also collects data when you visit other sites. For example, many websites have embedded Tweet buttons, which, even without Tweeting the website, alerts Twitter to the fact that you have visited the website. Twitter has admitted that it uses this information to recommend people to follow in Twitter.[66]

In 2013, Twitter acquired MoPub, a company that places ads within various mobile apps. This creates an advantage for Twitter because it allows advertisers not only to track Internet usage but also to track it across all devices. Data security experts have also raised security concerns about this type of tracking because hackers could obtain a multitude of information through MoPub.[67]

Twitter's track record on privacy, however, has been stellar to date. It allows users to opt out of tracking functions and respects the do not-track settings in browsers. Also, when government officials have attempted to subpoena Twitter users' data, Twitter has

[64] *Ibid.*
[65] *Supra* note 36 at 556.
[66] *Ibid.*
[67] *Ibid.*

resisted exposing the data. The Electronic Frontier Foundation has even named Twitter the best large technology company for protecting data.[68]

Users who tweet constitute an audience commodity that is sold to advertisers. The difference between the audience commodity on traditional mass media and on Twitter is that in the latter case the users are also content producers; there is user-generated content and the users engage in permanent creative activity, communication, community building and content-production. The fact that the users are more active on Twitter than in the reception of TV or radio content is due to the decentralized structure of the Internet, which allows many-to-many communication. Due to the permanent activity of the recipients and their status as prosumers, we can say that in the case of the Internet the audience commodity is a prosumer commodity. The category of the Internet prosumer commodity does not signify a democratization of the media towards a participatory or democratic system, but the total commodification of human creativity. Twitter users work for free, without payment; they generate surplus value by creating tweets and log data that are sold as commodity to advertisers that then target their ads to specific user groups. In order that capital accumulation can work on Twitter, the economic surveillance of user data is needed. Twitter surveillance is subsumed under the capitalist political economy.[69]

## 3.5 GOOGLE AND ITS SERVICES

A corporation founded in 1998 that dominates the Internet with its products and services. Google remains the most widely used search engine around the globe, and many of the company's communication and publishing tools and services continue to be among the market leaders, including its email service Gmail, video-sharing service YouTube, blogging platform Blogger, social media network Google+, and file-sharing service Google Drive. As Google which set out to "organize the world's information and make it universally accessible"— rose to become one of the world's most powerful technology companies, concerns about the company's protection of privacy also began to rise. While Google's web crawlers have been caching and indexing billions of web pages, the company has also been storing vast amounts of personal information on its servers. In 2007, the watchdog organization Privacy International rated Google as

[68] *Ibid.*
[69] *Supra* note 2 at 243.

"hostile" to privacy in a report that ranked Internet companies by how they handle the protection of personal data.[70]

Google manages the most popular Internet search engine, which generates revenue when users click or view advertising related to their searches. The company has a long history with privacy issues, and the researcher discuss major Google services — Gmail, Search, Street View, Buzz (and its successor, Google+).

### 3.5.1 Gmail

Gmail is Google's free, web-based and advertising-supported email service. When launched in early 2004 as an invitation-only beta release, it was an immediate success, offering users unprecedented storage capacity in exchange for receiving contextual ads. Gmail's ad engine automatically scans header information and the content of incoming and outgoing messages for key words provided by advertisers in advance. Despite this privacy-sensitive design, Google's decision to fund free storage by serving contextual ads proved quite controversial: users and consumer advocacy groups raised concerns over the lack of consent by non-subscribers, the impact of storage capacity on data retention (and hence government requests for data), and the prospect of Google someday modifying its approach and creating highly detailed user profiles based on the correlation of users' Gmail identities with their Google search behaviour. Despite numerous government investigations, no adverse actions were taken, and the controversy gradually faded without forcing any major change in Gmail's handling of ads.[71]

In 2004, in response to the launch of Gmail, thirty-one privacy and civil liberties organizations wrote a letter to Google's cofounders urging them to suspend the Gmail service until the company clarified its privacy protection policies and made its practices more transparent. The signers were concerned about Google's plan to scan the text of all incoming messages so that companies could place targeted ads based on keywords. In addition, they warned about the risks of misuse posed by the unlimited period for data retention.[72]

[70] *Supra* note 36 at 248.
[71] *Supra* note 49 at 1377.
[72] *Supra* note 36 at 248.

### 3.5.2 GOOGLE SEARCH

Unlike Gmail, Google Search attracted more sustained interest from privacy officials. Beginning in the final months of 2006, European and U.S. regulators challenged Google and its search engine competitors regarding the amount, sensitivity, and retention periods of the data collected for search ads and other purposes. Both consumer and regulatory concerns were spurred in part by two widely read news stories alerting the public to the data processing practices of their favourite search engines. Over the next several years, regulators and advocates called upon all search firms to offer greater transparency regarding their data practices, shorter data retention periods, and improved methods for anonymizing data after the retention period expired. In response, Google, Yahoo!, and Microsoft shortened data retention periods, sought to improve anonymization techniques, and began developing new compliance mechanisms. Soon, all of the major search firms were competing on privacy features for their search engine and browser offerings. Despite this heated competition, Google remained the leading search engine and moved ahead with a $3.1 billion acquisition of DoubleClick, overcoming objections on both antitrust and privacy grounds.[73]

With Search, the public grew alarmed when it learned that leading search engines were tracking their searches and collecting and storing sufficient information to attract the attention of law enforcement agencies and to permit inquisitive journalists to discover their "real-life" identities. Two interrelated design issues emerged: (1) how long search data should be retained before being deleted; and, (2) if it was anonymized instead of deleted, the proper method of anonymization. Google sought to achieve what it deemed the "right balance" between "privacy and other goals (like security, fraud prevention, and search improvements)" by retaining search logs for eighteen months and then "anonymizing" any data linking search terms to IP addresses by erasing the last octet of the IP address. To be sure, there is a trade-off between retaining data to improve search results and maintain security, and deleting or anonymizing search data to protect user privacy.[74]

Apart from google search privacy issues, researchers have unearthed that tech industry has failed to protect web browsers. Reuters reported a "newly discovered spyware effort" targeting users of Google's browser chrome. The spyware has been

[73] *Supra* note 49 at 1379.
[74] *Supra* note 49 at 1380.

pushed through at least 111 malicious or fake chrome browsers extensions, which have been downloaded some 32 million times. The report also said Google had taken off more than 70 extensions from its official web store last month after being alerted to their malicious nature by researcher at Awake security. These malicious extensions can take "screenshots, read the clipboard, harvest credential tokens stored in cookies or parameters, grab users' keystrokes (like passwords) says the report.[75]

### 3.5.3 GOOGLE STREET VIEW

Street View presents a more complex privacy scenario than either Gmail or Search. Launched initially in the United States in May 2007, Street View is an adjunct to Google Maps. Google Street View has been particularly controversial since inception of its launch. Street View allows users to view panoramic photographic images of locations and to zoom in and out on specific locations. Google has been collecting these images by dispatching a fleet of assorted vehicles equipped with specialized surveillance cameras to the areas that have been mapped. After being uploaded to the Internet, the photos are merged to create seamless panoramic views. Street View, initially introduced in a few U.S. cities, was quickly expanded and is now available for locations around the globe. The controversies surrounding Street View also highlight the challenges of confronting Google's data-collecting practices while establishing and affirming international safeguards for the protection of privacy.[76]

Lauren H. Rakower, an expert in technology law, has argued that Street View violates the international right to privacy as stated by the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. Several European countries, as well as Australia, temporarily banned the implementation of Street View, and citizens in several countries formed grassroots campaigns against dispatching Google's Street View fleet in their neighbourhoods. Protests increased after a European data protection agency discovered that Google has been collecting vast amounts of Wi-Fi data in addition to collecting images for Street View. In response, privacy advocates called for a Federal Communications Commission (FCC) investigation into whether Google's practices violated the federal Wiretap Act.[77]

[75] Sriram Srinivasan, "Google Chrome in Spying Spot" *The Hindu,* June 21, 2020.
[76] *Supra* note 36 at 248.
[77] *Ibid.*

Subsequently, more than twelve countries investigated Google's practices, and the company was ultimately charged with violating privacy laws in at least nine countries. In the class action suit Joffe v. Google, Inc., 729 F.3d 1262 (9th Cir. 2013), Google was sued for intercepting private communications from millions of users on unencrypted networks. The U.S. Ninth Circuit Court of Appeals affirmed the ruling that intercepting unencrypted Wi-Fi broadcasts violates the Wiretap Act. Google attempted to appeal to the U.S. Supreme Court. The Court declined to hear the case, however, affirming the lower court's decision. The company reached a $7 million settlement with the attorneys general of thirty-eight states and the District of Columbia over the Street View collection from unprotected Wi-Fi networks.[78]

Defending its practices, Google claimed that it collected the data by accident, yet it also admitted that it did not adequately protect the privacy of consumers. While Google stopped collecting Wi-Fi data through its Street View fleet, concerns about the company's data collection practices have not been alleviated. Indeed, the privacy issues are closely linked to the very nature of Google's operation and mission: The company "makes money because it harvests, copies, aggregates, and ranks billions of Web contributions by millions of authors," according to Siva Vaidhyanathan. Google collects information when users use its services; it copies and disseminates information about people that has been published on the Internet; and it continues to collect images for Street View, potentially exposing private views to the public. While Google has made it easier to control one's privacy settings by introducing a central portal under the "my account" settings, controlling the information that the company retains about individual users remains daunting. Google's privacy policies frequently change as the company evolves and develops new features such as Google Glass, opening up new privacy concerns.[79]

Significant recent challenges to Google's data collection and retention practices have come from European courts and policymakers. In Google Spain v. AEPD, (May 13, 2014) (Case C-131/12), the European Court of Justice ruled that European citizens have a right to request that commercial search firms, such as Google, that gather personal information for profit should remove links to private information when asked, provided the information is no longer relevant. The decision affirmed the "right to be

[78] *Ibid.*
[79] *Ibid.*

forgotten," which has been developed and implemented in the European Union (EU) and Argentina for the past decade. Subsequently, Google has had to respond to tens of thousands of requests to remove personal information from its index.[80]

The movement to establish international regulations to safeguard the protection of privacy by Google and other companies that collect vast amounts of user data continues to gain ground.[81]

### 3.5.4 BUZZ AND GOOGLE+

On February 9, 2010, Google launched Buzz, with great hopes for competing directly with Facebook in the SNS space. Towards that goal, Buzz included a feature that, "without prior notice or the opportunity to consent, Gmail users were, in many instances, automatically set up with 'followers' (people following the user)." In addition, after enrolling in Buzz, Gmail users were automatically set up to "follow" other users. Moreover, Google made this information publicly accessible to anyone viewing a user's profile. This decision to jump-start the Buzz social network by exploiting existing Gmail contact lists backfired, turning Buzz into a "danger zone" for investigative reporters, human rights activists, abuse victims, or anyone whose most frequent contacts were — and needed to remain — confidential. Google immediately created a war room and sought to resolve problems without delay; two days later, it adjusted Buzz's user interface by making it easier to opt-out of disclosing the lists of followers and people one follows, although the disclosure option was still pre-selected. In a blog post announcing further changes, Google sought to justify its decision to implement "auto-following" by noting, "we wanted to make the getting started experience as quick and easy as possible." But in response to customer concerns, Google introduced a new "auto-suggest" feature, which allowed users to review and approve follower suggestions based on their most frequent contacts.[82]

Buzz raised multiple privacy concerns that brought about its untimely demise. Buzz violated several FIPs and related privacy engineering requirements, including inadequate and misleading notice and lack of informed consent, and these deficiencies eventually forced Google to settle both a class action lawsuit and an FTC complaint.

[80] *Ibid.*
[81] *Ibid.*
[82] *Supra* note 49 at 1385.

Buzz also disregarded several design guidelines, including all five pitfalls of Lederer et al.[83]

Because Buzz was such a spectacular defeat for an otherwise successful and savvy company, it is worth pausing for a moment to ask a slightly different question: why did Google get Buzz so wrong? Danah Boyd suggests two reasons: first, Google launched Buzz as a "public-facing service inside a service that people understand as extremely private."[84] But this disrupted social expectations, or as Nissenbaum would say, violated contextual integrity. Second, "Google assumed that people would opt-out of Buzz if they did not want to participate." But this premise was flawed, as many unsuspecting users jumped into Buzz without understanding its information flows, became confused, and found it hard to exit, which only intensified their anxiety.[85]

## 3.6 COMPARATIVE ANALYSIS OF FACEBOOK, GOOGLE AND TWITTER's PRIVACY POLICIES REGARDING DATA COLLECTION

### Table 3.3: Privacy Policies Regarding Collection of Users Information

| Privacy Policies | Facebook | Google | Twitter |
|---|---|---|---|
| Information and Content users provide | √ | √ | √ |
| Networks and Connections | √ | √ | √ |
| Usage Information | √ | √ | √ |
| Information about transaction made | √ | √ | √ |
| Information from Devices | √ | √ | √ |
| Personal Information | √ | √ | √ |

**Source:** https://www.facebook.com/about/privacy (last visited on May, 30, 2022).
https://twitter.com/en/privacy (last visited on May, 30, 2022).
https://policies.google.com/privacy?hl=en-IN&fg=1 (last visited on May, 30, 2022).

[83] *Supra* note 49 at 1387.
[84] *Ibid.*
[85] *Id.* 1388.

Facebook's data policy does not explicate the specific types of data and information it gathers from its users; thus, it collects a large amount of data on its users. Facebook states that it collects "information and content users provide", including information from posts and information from users' messages and communications with other users. This can include information in or about the content users provide (e.g.) metadata, such as location of a photo or the date a file was created. Facebook collects information like users' religious views, political views, who you are "interested in" or your health. Facebook collects usage information about how users use its products, such the types of content that users view or engage with, the features users use, the action users take, the people or accounts users interact with the time, frequency and duration of users activities. Facebook also collect transactions information when users purchase any product or make a donation This includes user's credit or debit card number and other card information, other account and authentication information, and billing, shipping and contact details. The information collected by Facebook extends beyond a user's actions on Facebook to include information on the device or devices being used to access Facebook. This information details the device's operating system, hardware settings, device locations, and connection information, including network provider, browser type, language, time zone, IP address, and mobile phone number. Facebook also collects information from third-party partners and companies owned or operated by Facebook, such as Instagram.[86] Websites, apps and business that a user visits or use can send Facebook information through Facebook Technologies they use, including social plugins (such as the Like button), Facebook Login, Facebook API's and SDK's or the Facebook pixel or Instagram pixel. Facebook partners provide information about user's activities off Facebook – including information about users' device, website visited, purchases made, the ads users see and how users use Facebook services.[87]

Twitter also collects a large amount of its user's data in a similar manner of Facebook. From Twitter's privacy policies[88] it is clear that Twitter collects all the information shared by users with Twitter including account information (a username, password, email address, phone number); public information (user's time zone,

[86] *Supra* note 36 at 188.
[87] Facebook Privacy, *available at:* https://www.facebook.com/about/privacy (last visited on May 30, 2022).
[88] Twitter Privacy Policy, *available at:* https://twitter.com/en/privacy (last visited on May 30, 2022).

language). Twitter issues its advisory that users are responsible for their tweets, and other information provided by them through Twitter's services, and user should think carefully about what he/she makes public, especially if it is sensitive information. Twitter presumes that by publicly posting content/tweets, users are directing twitter to disclose that information as broadly as possible. To facilitate the fast global dissemination of tweets to people around the world, Twitter use technology like application programming interface (APIs) and embeds to make that information available to websites, apps, and others for their use. Twitter collects contact and address books, direct and non-public communication and payment information (credit or debit card number, card expiration date, CVV code, and billing address). Twitter presumes that if a user provides phone number, user agrees to receive text messages from Twitter to that number as user's country's law allows.[89]

Apart from information collected; Twitter also collects additional information of users like location information of users (IP address[90], device settings information), links[91], cookies[92], log data[93], receives information from ad partners as well as from third parties who are not Twitter's ad partners.

Google is too not lagging behind in collection of users vast information in overt and covert manner as Facebook and Twitter do. Google collects basic stuffs like language a user speaks, name, password, phone number, payment information, which ads user finds most useful, interest of users in people most, which YouTube videos user likes most. When a user is not signed in to a Google Account, Google collects information with unique identifiers[94] tied to the browser, application, or device a user is using. With the help of unique identifiers Google collects browser type, device type and settings, operating systems, mobile networks including carrier name and phone number and application version number including IP address. Google collects user's

[89] Twitter Privacy Policy, *available at:* https://twitter.com/en/privacy (last visited on May 30, 2022).
[90] Every device connected to the Internet is assigned a number known as an Internet Protocol (IP) address. These numbers are usually assigned in geographical blocks. An IP address can often be used to identify the location from which a device is connecting to the Internet.
[91] In order to operate services, Twitter keeps tracking of how users interact with links across its services. This includes links in emails Twitter send users and links in Tweets that appear on other websites or mobile applications.
[92] A cookie is a small piece of data that is stored on your computer or mobile device.
[93] The Log Data includes information such as your IP address, browser type, operating system, the referring web page, pages visited, location, your mobile carrier, device information, search terms etc.
[94] A unique identifier is a string of characters that can be used to uniquely identify a browser, app or device.

location information with the help of GPS, IP address, Sensor data from user's device, information about things near user's device, such as WI-FI access points, cell towers, and Bluetooth-enabled devices. In some circumstances, Google also collects information about a user from publicly accessible sources. For example, if a user's name appears in a local newspaper, Google Search engine may index that article and display it to other people if they search for this user's name. Google also collects users' information from its business partners, security partners, advertising partners.[95]

## 3.7 CONCLUSION

Every social media website has a privacy policy. The purpose of a privacy policy is to outline how organizations will collect, maintain, and share user data. When an organization does not notify users in clear manner about who, how and why is collecting the data, the user is unable to enjoy his/her right to privacy.

The preceding discussion on nature of privacy policies of social media conveys that privacy policies/Terms of use/User Agreement are written in ambiguous, vague and confusing language which undermines the effectiveness and purpose of privacy policy. Privacy policies tend to be long boring document with ambiguous and misleading language; one of the reasons behind not reading privacy policies of social media by the users. Often organizations write the privacy policy in a way that protects the organization more than the user.

Web Tracking, self-regulated mode of operation, standard form of contract between social media sites and users are some other issues associated with social media. Targeted advertising is one of the main sources of revenue generation of almost all the social networking sites / apps. Facebook coerces users into agreeing to the use of their personal data and collected user behaviour data for economic purposes. If a user does not agree to the privacy terms that makes targeted advertising possible, user is unable to use the platform. Twitter and Google also use targeted advertising for revenue generation.

News Feed, Becon, Facebook Apps, Photo sharing, Facial Recognition Technology and many other controversial features of Facebook show that Facebook involves in accumulation of money in deceptive manners. Google and its product –

[95] Google Privacy & Terms, *available at:* https://policies.google.com/privacy?hl=en-IN&fg=1 (last visited on May 30, 2022).

Gmail, Google Search Engine, Street View, Buzz all have witnessed privacy issues. Twitter's business mode is also based on targeted advertising.

**One of the hypotheses of the present study was "Privacy policies of social media are ambiguous, coercive and deceptive".**

**On the basis of the above discussion and concluding remarks, the researcher has reached to the conclusion that "Privacy policies of social media are ambiguous, coercive and deceptive". Hence, the hypothesis is proved.**

# CHAPTER-IV
# PRIVACY LAWS & SOCIAL MEDIA: INTERNATIONAL PERSPECTIVE

# CHAPTER IV
# PRIVACY LAWS & SOCIAL MEDIA: INTERNATIONAL PERSPECTIVE

The right to privacy has been recognized and accepted all over the world as an essential human right. Privacy is an important component of human personality.

Human rights are codified in international law by means of international and regional conventions. Privacy finds a prominent place in each of these rights regimes. Further, international and regional human rights institutions have consistently applied the right to protect individuals from unlawful interference in their private space and family life.

The human rights movement came to a precipice when a concerted attempt was made to codify such rights that are inalienable to man. The emergence of the United Nations and the inclusion of human rights as a major area of international law and politics resulted in human rights jurisprudence gaining greater force in municipal and international judicial forums.

The right to privacy has been recognized across jurisdictions along with international and regional conventions. The importance of privacy in this regard is evidenced by its virtual universal impetus in every human right related instrument or dialogue.

## 4.1 PRIVACY IN INTERNATIONAL HUMAN RIGHT LAW

Article 12[1] of the Universal Declaration of Human Rights (1948) and Article 17[2] of the International Covenant on Civil and Political Rights protect individuals' privacy, honour and reputation, their families, home, and correspondence against any arbitrary interference.

[1] The Universal Declaration of Human Rights, 1948, art. 12.
It states as follows:
"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."

[2] The International Covenant on Civil and Political Rights, 1966, art. 17.
It states as follows:
"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."

The Human Rights' documents include an individual's right to privacy on the digital communications without any arbitrary interference. Article 17 also implies in principle that individuals have the right to share information and ideas with one another without interference by the State, secure in the knowledge that their communication will reach and be read by the intended recipients alone.[3]

A similar construct is employed in the specific context of migrant worker rights as well in Article 14 of the International Convention on the Protection of the Rights of All Migrant Workers and Members of their families[4] from arbitrary interference with their family life and privacy.

Article 16 of the Convention on the Rights of Child and Article 22 of the Convention on the Rights of Persons with Disabilities also specifically seek to establish protection for privacy of children and persons with disabilities.

The right to privacy as a human right is firmly established in international law conventions. Therefore, the position of privacy in the catena of human rights is universally accepted.

## 4.2 PRIVACY IN REGIONAL HUMAN RIGHTS CONVENTIONS

Article 8[5] of the European Convention on Human Rights (ECHR) lays down the basis for one of the most progressive privacy regimes in the world.

Article 11[6] of the American Convention on Human Rights has given privacy its due place in its framework.

[3] UN General Assembly, *Promotion and protection of human rights and fundamental freedoms while countering terrorism,* UN Doc A/69/397 (September 23, 2014). *available at*: https://docs.google.com/document/d/18U1aHmKx9jfDQjCZeAUYZdRjl6iF4QjuS_aJO2Uy7NY/edit?pli=1# (last visited on May 30, 2022).

[4] The International Convention on the Protection of the Rights of All Migrant Workers and Members of their families, 1990, art. 14 read as – "No migrant worker or member of his or her family shall be subjected to arbitrary or unlawful interference with his or her privacy, family, 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."

[5] European Convention on Human Rights, 1953, art. 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."

[6] The American Convention on Human Rights, 1969, art. 11. "1. Everyone has the right to have his honor 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 honor or reputation. 3.Everyone has the right to the protection of the law against such interference or attacks."

The African Charter of Human and People's Rights (ACHPR) does not explicitly set out the right to privacy, but Article 18[7] attaches particular importance to the State's duty to protect family life.

The prominent position of privacy in human rights jurisprudence is reflected by its acceptance in multiple regional instruments for human rights protection. This established a rich source of law for the formulation of a specific privacy protection regime.

## 4.3 DATA PROTECTION AND PRIVACY ISSUES IN SOCIAL MEDIA

New technologies permit easy dissemination and use of the information. Current ICT allows individuals to share (sometimes unknowingly) their personal preferences and behaviour information on an unprecedented scale. This could lead to people losing control of personal information. Web 2.0[8] is an increasing part of our daily lives. One of its more popular examples is social media. One of the most controversial issues in relation to social media websites is their data processing and respect for privacy and personal data.[9]

The problem with privacy issues on SNS is that these companies are not entirely regulated the same way as Internet service providers (ISPs), both generally and in relation to privacy, on how they manage the data they collect. It is therefore worth looking at the broader privacy and data protection policy environment in Western societies that shape the possibilities and conditions for data manipulation and protection in the context of digital media.[10]

In order to explore the types of privacy issues that social media raises, it is useful to consider what the concept of 'data protection' actually is and how it has become

[7] The African Charter of Human and People's Rights, 1979, art. 18. 1."The family shall be the natural unit and basis for 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 of 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 women 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."

[8] Web 2.0 is the second stage of development of the internet, characterized especially by the change from static web pages to dynamic or user-generated content and the growth of social media.

[9] Dr. Paul Lambert, *A User's Guide to Data Protection* 557 (Bloomsbury Professional Ltd, RH, 2016).

[10] Monroe E. Price, Stefaan G. Verhulst and Libby Morgan et.al. (eds.), *Routledge Handbook of Media Law* 474-475 (Routledge, New York, 2013).

manifested within special legal regulation. Data protection applies to individuals and their rights that relate to the use and disposal of their data in connection with their personality. In recent years, these rights have become increasingly important as technology has enabled the collecting, storing, and conciliation of large pools of data. The aim of data protection law is the protection of privacy in relation to data.[11]

Data protection aims to protect the privacy and personal information of individuals. It provides a regulatory protection regime around personal information privacy or personal data. The data protection legal regime governs when and how organizations may collect and process personal data.

Data privacy laws systematically regulate the use of information about people. They are also known as 'data protection' or 'fair information', and the individuals affected are sometimes called 'data subjects'. Data privacy laws essentially comprise a set of enforceable data privacy principles based on the 'life cycle' of personal data (collection, accuracy, security, use, disclosure, access, deletion etc.) coupled with an enforcement structure backed by legal measures requiring compliance. Enforcement usually involves a data privacy authority often called a 'Data Protection Authority' (DPA) or 'Privacy Commissioner', but often involves other enforcement authorities as well.[12]

## 4.4 HISTORY OF DATA PROTECTION LEGISLATION

In this section, the researcher has discussed the history of data protection legislation in the world which was an attempt to protect the privacy of individuals by different nations.

### 4.4.1 THE YOUNGER COMMITTEE REPORT

In 1972, the UK Government set up the Younger Committee, which was tasked a broad remit to consider whether legislation was needed to protect individuals and organizations from intrusions into their personal privacy. The Younger Committee Report[13] concluded that the general public's principal concern was that the government

[11] Laura Scaife, *Handbook of Social Media and the Law* 238 (Informa Law from Routledge, New York, 2015).
[12] Graham Greenleaf, *Asian Data Privacy Laws – Trade and Human Rights Perspective* 5-6 (Oxford University Press, United Kingdom, 2014).
[13] Younger Committee (Report of the Committee on Privacy), Cmnd 5012 (1972). London: HMSO in Laura Scaife, *Handbook of Social Media and the Law* 242 (Informa Law from Routledge, New York, 2015).

might have the ability to construct a central computer databank containing their information. The report recommended ten principles for the use of computers for the processing of personal data - the forerunners of the present 'data protection principles.'

In response to the Younger Committee's Report, the government produced a White Paper,[14] which concluded that 'the time has come when those who use computers to handle personal information, however responsible they are, can no longer remain the sole judges of whether their own systems adequately safeguard privacy.

### 4.4.2 THE LINDOP REPORT

Three years after the publication of its White Paper, the government commissioned the Lindop Report which looked in more detail at the practical aspects of data protection and the mechanics of how it could be implemented. One of the Lindop Report's key recommendations was that a Data Protection Authority should be created and that Codes of Practice for the processing of data should be drafted and adopted by different sectors.

### 4.4.3 THE OECD GUIDELINES (1980)

From the start of the 1980s the non-binding and the first binding international agreement, the Council of Europe Data Protection Convention, both embodied substantially similar privacy principles expressed in somewhat different language. The Organization for Economic Co-operation and Development (OECD) Privacy Guidelines (1980) were an early influence on the development of data privacy laws. The OECD Guidelines on *the Protection of Privacy and Transborder Flow of Personal Data* were one of the first formulations of a comprehensive set of information privacy principles.[15]

Eight principles, namely Collection Limitation Principle, Data Quality Principle, Purpose Specification Principle, Use Limitation Principle, Security Safeguards Principle, Openness Principle, Individual Participation Principle, and Accountability Principle, were also adopted by the Organization for Economic Cooperation and Development (OECD) in order to regulate the trans-border data flow.[16]

---

[14] *Ibid.*
[15] *Supra* note 12 at 5.
[16] Organization for Economic Cooperation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (October 1, 1980). *available at*: http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html (last visited on May 30, 2022).

The Guidelines are proposed as minimum standards for the protection of privacy and individual liberties and the advancement of free flows of personal data. They apply to both the public and private sectors.

### 4.4.4 THE DATA PROTECTION ACT, 1984

There was significant debate in the UK about the Convention as the government was concerned that it might impact upon business activity and commerce and wanted to ensure that the UK met international standards to enable data to be transferred. In 1982, a Bill was introduced, which after passing through Parliament became the Data Protection Act 1984. The 1984 Act contained the provisions of the Younger Report as reflected in the Council of Europe Convention.

The 1984 Act established new rights for individuals to know if an organization was processing personal data about them and the right to have a copy of the information and as recommended in the Lindop Report, it established the office of Data Protection Registrar who had powers to enforce the regime. For the first time, individuals had the possibility of complaining to the Registrar and then to the newly established Data Protection Tribunal should their complaint proceed.[17]

---

Eight Principles are as follows:

(a) Collection Limitation Principle: Personal data should be collected in a very limited manner. Indeed, while collecting personal data, lawful and fair means should be adopted. In appropriate cases, it should be obtained with the knowledge and consent of the data subject.

(b) Data Quality Principle: It is necessary that Personal data should be relevant to the intended purposes and, should be accurate, complete and kept up-to-date.

(c) Purpose Specification Principle: At the time of data collection, purpose should be specified and should be used for that purpose only.

(d) Use Limitation Principle: The consent of the data subject or the authority of law is required to disclose the personal data. Same consent or authority is necessary if the data is used for unintended purposes.

(e) Security Safeguards Principle: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

(f) Openness Principle: It is required that an individual should have a way to know the existence, nature, and, purposes of personal data. There should also be a certain means to know the identity and residence of the data controller. In other words, there must be openness in developments, practices and policies of collecting the personal data.

(g) Individual Participation Principle: An individual should have the right to confirm that whether a data controller has data relating to him or not. Such confirmation should be communicated to him within reasonable time and in reasonable manner. If the data controller denied the request, then it becomes necessary on his part to give reasons for such denial. Furthermore, the individual should have the right to challenge the denial. Besides, the individual should have the right to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed, or amended.

(h) Accountability Principle: Under this principle, a data controller should adopt certain measures to give effect to the above said principles.

[17] *Supra* note 12.

### 4.4.5 THE 1995 EU DIRECTIVE

The European Union, which had tended to leave human rights issues to the Council of Europe, became involved in data privacy in the early 1990s, and by 1995 adopted the general data protection directive 95/46/EC (the 'EU Directive').[18]

The Directive 95/46/EC of the European Parliament and of the Council was passed to balance the free flow of personal data within European Union member countries and the right to privacy of European citizens. The directive prohibited the transfer of the individuals' information to a third country that doesn't have an adequate law on privacy protections.[19] It also contains provisions ensuring the principles of openness, access and correction, collection limitation and finality, accuracy, security, and enforcement or redress. The Directive prohibits European Union (EU) member states from collecting data that reveal an individual's ethnic origin, race, political conviction, religious beliefs, or health and sexuality.[20]

Considering the implications of the new technologies, the European Commission concluded that the Directive of 1995 needed to be amended and updated. In 2002, E-privacy directive was drafted to provide privacy in the new digital world. It covered those areas which were not in the domain of the directive of 1995.

### 4.4.6 THE DATA PROTECTION ACT, 1998

The history of data protection reveals that the implications of new technologies like social media compelled the concerned governments to update their data protection legislations. Following this trend, the UK enacted 'The Data Protection Act 1998' commenced on 1 March 2000 to serve the needs of the society with changing dimensions of technology.

The DPA 1998 provides details as to what constitutes fair processing and identifies the information that must be given to Data Subjects not only where the

[18] *Supra* note 12.
[19] Article 25 of Directive 95/46/EC of the European Parliament and of the Council, *The protection of individuals with regard to the processing of personal data and on the free movement of such data* (October 24, 1995). *available at*: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML (last visited on May 30, 2022).
[20] Art. 8(1) of Directive 95/46/EC of the European Parliament and of the Council, *The protection of individuals with regard to the processing of personal data and on the free movement of such data* (October 24, 1995). *available at*: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML (last visited on May 30, 2022).

personal data is obtained directly from the Data Subjects but also when it is obtained indirectly. It also refers to the times at which this information needs to be given.[21]

Schedule 1 Part 1 of the DPA 1998 sets out the Data Protection Principles. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless at least one of the conditions in Sch 2 is met, and in the case of sensitive personal data, at least one of the conditions in Sch 3 is also met.

There are eight Data Protection Principles to be complied with by all Controllers, which can be summarized as follows:

(1) fairly and lawfully processed;[22]

(2) processed for limited purposes;[23]

(3) adequate, relevant and not excessive;[24]

(4) accurate and up to date;[25]

(5) not kept for longer than is necessary;[26]

(6) processed in line with Data Subject Rights;

(7) secure; and

(8) not transferred to other countries without adequate protection.

The sixth Data Protection Principle states that personal data must be processed in line with the Data Subject's rights. The rights of Data Subjects can be summarized in various sections of DPA 1998.[27]

---

[21] Data Protection Act, 1998 a*vailable at*: https://www.legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf (last visited on May 30, 2022).

[22] *First Data Protection Principle* - The collection and processing must be fair and transparent. It must, therefore, be in a manner that is not covert or deceptive.

[23] *Second Data Protection Principle* - The second Data Protection Principle states that personal data must be processed for limited purposes.

[24] *Third Data Protection Principle* **-** The third Data Protection Principle states that personal data must be adequate, relevant, and not excessive.

[25] *The fourth Data Protection Principle* states that personal data must be accurate and up to date. The personal data must be correct and accurate. Given that personal data can become out of date, and consequently increase the risk of adverse consequences for the individual Data Subject, there is an obligation to ensure that the personal data is kept up to date. This means continuing assessing the data and updating, correcting or deleting it as appropriate. It also implies a finite end to processing activities.[25]

[26] *The fifth Data Protection Principle* states that personal data must be not kept for longer than is necessary. Once the purpose is accomplished, the need is over and there does not continue to be a current purpose continuing for to keep and process the personal data. It must be kept no longer than necessary in relation to the original collection and processing purpose.

[27] right of access (DPA 1998, s 7);
right to establish if personal data exists (Data 1998, s 7 (1) (a));
right to be informed of the logic in automatic decision taking (DPA 1998, s 7(1)(d));
right to prevent processing for direct marketing (DPA 1998, s 11);
right to prevent automated decision taking (DPA 1998, s 12 A);

The seventh Data Protection Principle states that personal data must be secure.

This is critically important and is increasingly emphasized with the significant number of official and commercial data breach and data loss incidents. In addition, there is an increasing emphasis that organizations should not only the ICO but also individual Data Subjects in the event of data breach. The latter can be justified if it would be necessary for individuals to change passwords, etc, in order to minimize damage, loss or distress from the misuse of the personal data the subject of the breach.[28]

The eighth data protection principle states that personal data must not to be transferred to other countries without adequate protection.

### 4.4.7. THE ROME MEMORANDUM

In March 2008, the Berlin International Working Group on Data Protection in Telecommunications adopted a memorandum[29] that analyzed the risks for privacy and security posed by social networks and provided guidelines for regulators, providers and users Recommendations of the Rome Memorandum are as follows[30]:

right to compensation (DPA, s 13);
right to rectify inaccurate data (DPA 1998, s 14);
right to rectification, blocking, erasure and destruction (DPA 1998, s 14);
right to complain to ICO (DPA 1998, s 42);
right to go to court (DPA 1998, s 15).

[28] Dr. Paul Lambert, *A User's Guide to Data Protection* 74 (Bloomsbury Professional Ltd., RH16, 2016).

[29] Report and Guidance on Privacy in Social Network Services, International Working Group on Data Protection in Telecommunication 43rd meeting, 3-4 March 2008, Rome (Italy). Available at: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2008/2008-Rome_Memorandum-en.pdf (last visited on May 30, 2022).

[30] The Rome Memorandum recommended the following:

- More transparency and open information for uses:
  - Information must be tailored to the specific needs of the targeted audience (especially for minors) to allow them to make informed decisions;
  - Information of users should also refer to third party data.
- To provide privacy policies.
- To introduce the creation and use of pseudonymous profiles as an option.
- To live up to promises made to users to foster and maintain user trust through clear and unambiguous information about how their information will be treated by the service provider, specifically when it comes to sharing personal data with third parties.
- To introduce privacy-friendly default settings to improve user control over use of profile data:
  - *Within the community*, e.g. allow restriction of visibility of entire profiles, and of data contained in profiles, as well as restriction of visibility in community search functions. Tagging of photos (i.e. the addition of links to an existing user profile or the naming of depicted persons) should be bound to the data subject's prior consent.
  - *Create means allowing for user control over third party use of profile data* – vital in particular to
    address risks of ID theft.

On a self-regulatory and voluntary basis, the European Union has pursued the regulation of SNS in relation to vulnerable groups, in particular youth and children, through its Safer Internet Plus Programme. In July of 2008, the Programme initiated a public consultation on child safety and social networking, the results of which were summarized and published in a related report[31].

Following this, the Safer Social Networking Principles[32] were issued in February 2009, and the first self-regulatory agreement to follow these principles was signed by the main social networks. The Commission assessed the implementation of this agreement on Safer Internet Day in 2010, and again in 2011, and stated its disappointment with the ways in which SNS had failed to protect the privacy of underage users. This is a major blow to many years of efforts to develop self-regulatory regimes for SNS as an answer to the issues raised by the risks faced especially by younger users, who make up the majority of their users.

### 4.4.8 ARTICLE 29 WORKING PARTY AND EUROPE

Article 29 of the EU Directive creates a "Working Party on the Protection of Individuals with regard to the Processing of Personal Data' (the 'Article 29 Working

- *Allow for user control over secondary use of profile and traffic data, e.*g. for marketing purposes, as a minimum: opt-out for general profile data, opt-in for sensitive profile data (e.g. political opinion, sexual orientation) and traffic data.
- *Comply with user rights recognized in national, regional and international privacy frameworks,* including the right of data subjects to have data – which may well be entire profiles – erased in a timely manner.
- *Address the issue that may arise in cases of a takeover or merger of a social network service company* – introduce guarantees for users that new owner will maintain privacy (and security) standard.

- To adopt appropriate complaint handling mechanisms, where they do not already exist, for users of social networks, but also with respect to third-party personal data.
- To improve and maintain the security of information systems by using recognized best practices in planning, developing, and running social networks service applications, including independent certification.
- To devise and/or further improve measures against illegal activities, such as spamming and ID theft.
- To offer encrypted connections for maintaining user profiles, including secured log-in.
- That social network providers acting in different countries or even globally should respect the privacy standards of the countries where they operate their services.

[31] European Commission, Public Consultation on Online Social Networking: Summary Report, Brussels: EC (2008). *available at:* http://ec.europa.eu/information_society/activities/sip/docs/pub_consult_age_rating_sns/summaryreport.pdf (last visited on May 30, 2022).

[32] European Commission, *The Safer Social Networking Principles for EU, Brussels: EC* (2009). *available at:* ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf (last visited on May 30, 2022).

Party') comprised primarily of the representatives of each EU member state's DPA. The EU Directive was the first international instrument to control exports of personal data to countries not bound by the same data privacy rules (in this case, non-EU/EEA countries). Article 25 permits such exports from EU member states 'only if … the third country in question ensures an adequate level of protection'. As yet, the EU has only made positive 'adequacy' assessments in relation to 11 jurisdictions as a whole, a minority of which are of economic or political significance. No Asian country has as yet received a positive adequacy assessment from the EU. India is known to have been assessed at least twice (in 2010 and 2013), but no recommendation of adequacy has gone forward from the EU Commission to the Article 29 Working Party.[33]

### 4.4.9 EUROPEAN UNION GENERAL DATA PROTECTION REGULATION

On 25 January 2012, the European Commission unveiled a draft European General Data Protection Regulation[34] that will supersede the Data Protection Directive after noting that as a result of modern technology, with EU Commissioner Vivian Reading specifically noting social media as a key example, the 1995 Directive was unable to meet the increasing demands placed upon privacy protection in the digital age.[35]

The European Commission plants to unify data protection within the European Union with a single law, the General Data Protection Regulation (DPR). The current EU Data Protection Directive 95/46/EC does not consider important aspects like globalization and technological developments like social networks and cloud computing sufficiently, and the Commission determined that new guidelines for data protection and privacy were required.

A proposal for a regulation was released on 25 January 2012. Subsequently, numerous amendments have been proposed in the European Parliament and the Council of Ministers. The key changes relate to:

- Strengthening the "right to be forgotten" to help people better manage data protection risks online. When individuals no longer want their data to be

[33] *Supra* note 12.
[34] Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing Data and on the Free Movement of such Data, Brussels, 25.1.2012, COM (2012) Final 2012/0011 (COD), European Council.
[35] The European Commission issued a consultation paper titled '*Safeguarding Privacy in a Connected World'*(January 25, 2012). *available at:* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_9_en.pdf (last visited on May 30, 2022).

processed and there are no legitimate grounds for retaining it, the data will be deleted. The rules are about empowering people, not about erasing past events or restricting the freedom of the press.

- Guaranteeing easy access to one's own data.
- Establishing a right for individuals to freely transfer personal data from one service provider to another (data portability).
- Ensuring that consent must be given explicitly by individuals when it is required for certain types of data processing.
- Increasing the responsibility and accountability of those processing data by introducing data protection officers for companies with over 250 employees, and the principles of 'privacy by default' and 'privacy by design' to ensure that individuals are informed in an easily understandable way about how then data will be processed.

On May 25th, 2018, the European Data Protection Regulation came into effect in order to harmonize data privacy laws across Europe.[36] This regulation replaced the Data Protection Directive of 1995. European Union General Data Protection Regulation aims to:[37]

- lay down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
- protect fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.
- provide free movement of personal data within the Union.

This Regulation applies to both public authorities and private entities processing or controlling the individuals' personal information. 'Personal data' means any information relating to an identified or identifiable natural person.[38]

[36] General Data Protection Regulation (GDPR). *available at*: https://gdpr-info.eu/ (last visited on May 30, 2022).
[37] General Data Protection Regulation, art. 1, *available at*: https://gdpr-info.eu/art-1-gdpr/ (last visited on May 30, 2022).
[38] General Data Protection Regulation art. 4(1).
It provides: 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

In *Patrick Breyer v. Bundesrepublik Deutschland*[39] the European Court of Justice held that 'dynamic IP (internet protocol) address' is 'personal information' when the online media services provider's (e.g., provider of a website) legal access to the additional data held by the internet service provider enables the former (i.e., website provider) to identify the person who has accessed its (website provider) publicly accessible website.

### 4.4.10 EU GDPR Vs. UK GDPR

The General Data Protection Regulation or the GDPR is an (EU) regulation designed to protect the privacy rights of individuals in the European Economic Area. It is intended to be an overarching privacy regulation for all EU Member States and replaces prior EU privacy regulations and goes even further than benchmark United States privacy laws governing health care and educational records, such as the Health Insurance Portability and Accountability Act (HIPAA) and the Family Education Rights and Privacy Act (FERPA).

On January 1, 2021, the United Kingdom's UK GDPR rules became effective. The UK GDPR absorbs the privacy compliance requirements of the Data Protection Act. EEA's GDPR and combines them with the requirements of the UK's Data Protection Act.[40]

## 4.5 GDPR COVERS SOCIAL MEDIA PROVISIONS

The initial provisions of GDPR refer to the context of the GDPR, namely, the subject matter and objectives (Article 1); material scope (Article 2); and territorial scope (Article 3).

The GDPR applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system (Article 2(2)). Matters not covered or included are referred to in Article 2(3).

[39] *Patrick Breyer v. Bundesrepublik Deutschland,* C-582/14 ECLI:EU:C:2016:779.
[40] https://ethics.berkeley.edu/privacy/general-data-protection-regulation-gdpr-and-uk-gdpr (last visited on May 30, 2022).

An important case may be Google Spain[41] and Google Case C-131/12 in the ICJ. This is a reference for a preliminary ruling from the Audiencia Nacional (Spain). It specifically relates to the following:

- interpretation of Arts 2(b) and (d), 4(l)(a) and (c), 12(b) and 14(a) of the DPD; and
- Art 8 of the charter of Fundamental Rights of the EU (OJ *2000* 364, p 1);
- concept of establishment on the territory of a Member State;
- relevant criteria;
- concept of 'use of equipment situated on the territory of a Member State';
- temporary storage of information indexed by internet search engines;
- right to erasure and blocking of data.

The Court of Justice held that:

'Article 2(b) and (d) of Directive 95/46/EC ... are to be interpreted as meaning that, first, the activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as "processing of personal data" within the meaning of Article 2(b) when that information contains personal data and, second, the operator of the search engine must be regarded as the "controller" in respect of that processing, within the meaning of Article 2(d).

Article 4(1)(a) of Directive 95/46 is to be interpreted as meaning that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State'.

The recent Weltimmo[42] case also refers to jurisdiction issues, holding that a SA can sometimes have jurisdiction even over organisations located elsewhere. DPD Article 28(6) provides:

[41] *Google Spain SL and Google Inc v Agencia Espanola de Protection de Datos (AEPD) and Mario Costeja Gonzdtez*, C-J 31/12,13 May 2014.
[42] *Weltimmo sro v Nemzeti Adatvidelmi es Infonndcidszabadsdg Hatosag,* Court of Justice, C-230/14, 1 October 2015.

'Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.'

DPD Article 4 states:

'Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:
(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable.'

The Court of Justice held that:

'1. Article 4(1)(a) of the DPD must be interpreted as permitting the application of the law on the protection of personal data of a Member State other than the Member State in which the controller with respect to the processing of those data is registered, in so far as that controller exercises, through stable arrangements in the territory of that Member State, a real and effective activity - even a minimal one - in the context of which that processing is carried out.

In order to ascertain, in circumstances such as those at issue in the main proceedings, whether that is the case, the referring court may, in particular, take account of the fact (i) that the activity of the controller in respect of that processing, in the context of which that processing takes place, consists of the running of property dealing websites concerning properties situated in the territory of that Member State and written in that Member State's language and that it is, as a consequence, mainly or entirely directed at that Member State, and (ii) that that controller has a representative in that Member State, who is responsible for recovering the debts resulting from that activity and for representing the controller in the administrative and judicial proceedings relating to the processing of the data concerned.

By contrast, the issue of the nationality of the persons concerned by such data processing is irrelevant.

2. Where the supervisory authority of a Member State, to which complaints have been submitted in accordance with Article 28(4) of DPD, reaches the conclusion that the law applicable to the processing of the personal data concerned is not the law of that Member State, but the law of another Member State, Article 28(1), (3) and (6) of that directive must be interpreted as meaning that that supervisory authority will be able to exercise the effective powers of intervention conferred on it in accordance with Article 28(3) of that directive only within the territory of its own Member State. Accordingly, it cannot impose penalties on the basis of the law of that Member State on the controller with respect to the processing of those data who is not established in that territory, but should, in accordance with Article 28(6) of that directive, request the supervisory authority within the Member State whose law is applicable to act.

3. DPD must be interpreted as meaning that the term "adatfeldolgozds" (technical manipulation of data), used in the Hungarian version of that directive, particular in Articles 4(l)(a) and 28(6) thereof, must be understood as having the same meaning as that of the term "adatkezeles" (data processing).'

### 4.5.1 DATA PROTECTION PRINCIPLES

Chapter II refers to the Data Protection Principles. Article 5 of the new GDPR relates to principles relating to personal data processing.[43]

[43] Principles relating to the processing of personal data *available at*: https://gdpr-info.eu/art-5-gdpr/ (last visited on May 30, 2022).
Article 5, GDPR read as Personal data shall be:
processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'); collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving; purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation'); adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'); accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy'); kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation'); processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

The Controller shall be responsible for and be able to demonstrate compliance with Article 5(1) ('accountability' principle) (Article 5(2)).

Article 6 of the new GDPR refers to the lawfulness of processing.[44]

Member States may maintain or introduce more specific provisions to adapt the application of the rules of the GDPR with regard to the processing of personal data for compliance with Article 6(1)(c) and (e) by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX (Article 6(2)).

The basis for the processing referred to in Article 6(1)(c) and (e) of must be laid down by: EU law, or Member State law to which the Controller is subject.

The purpose of the processing shall be determined in this legal basis, or as regards the processing referred to in Article *6(1)*(e), shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller. This legal basis may contain specific provisions to adapt the application of rules of the GDPR, *inter alia,* the general conditions governing the lawfulness of data processing by the Controller, the type of data which are subject to the processing, the Data Subjects concerned; the entities to, and the purpose for which the personal data may be disclosed; the purpose limitation; storage periods, and processing operations and processing procedures including measures to ensure lawful and fair processing,

[44] Article 6, GDPR, Lawful Processing *available at*: https://gdpr-info.eu/art-6-gdpr/ (last visited on May 30, 2022).
*Article* 6(1) *provides that processing of personal data shall be lawful only if and to the extent that at least one of the following applies:*

- *the Data Subject has given consent to the processing of their personal data for one or more specific purposes;*
- *processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract;*
- *processing is necessary for compliance with a legal obligation to which the Controller is subject;*
- *processing is necessary in order to protect the vital interests of the Data Subject or of another natural person;*
- *processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller;*
- *processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of personal data, in particular where the Data Subject is a child. This (bullet) shall not apply to processing carried out by public authorities in the performance of their tasks (Article* 6(1)).

such as those for other specific processing situations as provided for in Chapter IX EU law or the law of the Member State must meet an objective of public interest and be proportionate to the legitimate aim pursued (Article 6(3)).

Where the processing for a purpose other than that for which the personal data have been collected is not based on the Data Subject's consent or on an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the Controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

- any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
- the context in which the personal data have been collected, in particular regarding the relationship between Data Subjects and the Controller;
- the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9 or whether data related to criminal convictions and offences are processed, pursuant to Article 10;
- the possible consequences of the intended further processing for Data Subjects;
- the existence of appropriate safeguards, which may include encryption or pseudonymisation (Article 6(4)).

### 4.5.2 CONSENT AND SOCIAL MEDIA

Article 7 of the new GDPR refers to conditions for consent as follows. Where processing is based on consent, the Controller shall be able to demonstrate that the Data Subject has consented to the processing of their personal data (Article 7(1)).[45]

If the Data Subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent must be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of the declaration which constitutes an infringement of the GDPR shall not be binding (Article 7(2)).

[45] Article 7, GDPR, Conditions for Consent, *available at:* https://gdpr-info.eu/art-7-gdpr/ (last visited on May 30, 2022).

The Data Subject shall have the right to withdraw their consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the Data Subject shall be informed thereof. It shall be as easy to withdraw consent as to give consent (Article 7(3)).

When assessing whether consent is freely given, utmost account shall be taken of the fact whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract (Article 7(4)).

### 4.5.3 RIGHTS OF DATA SUBJECTS IN GDPR

Chapter III of the GDPR refers to the rights of Data Subjects. These rights have been mentioned in different section of GDPR.[46]

### 4.5.4 JURISDICTION AND SOCIAL MEDIA

One of the developing and more contentious areas of internet liability relates to issues of service provider liability. There is a claim often advanced by some service providers, that they are not liable to the EU data protection regime if the companies and or parent companies are located in the US. Effectively, they are claiming to be exempt from having to comply with EU law in relation to EU citizens in Europe, and the personal data of those citizens. Other companies, however, are happy to indicate a willingness to comply with EU data protection rules. Facebook, for example, indicated

[46] Rights of Data Subjects, Chapter III, GDPR, *available at:* https://gdpr-info.eu/chapter-3/ (last visited on May 30, 2022).

- *right to transparency (Article 5; Article 12);*
- *right to prior information; directly obtained data (Article 13);*
- *right to prior information: indirectly obtained data (Article 14);*
- *right of confirmation and right of access (Article 15);*
- *right to rectification (Article 16);*
- *right to erasure (Right to be Forgotten) (RtbF) (Article 17);*
- *right to restriction of processing (Article 18);*
- *notification re rectification, erasure or restriction (Article 19);*
- *right to data portability (Article 20);*
- *right to object (Article 21);*
- *rights re automated individual decision making, including profiling* (Article 22);
- DPbD (Article 25);
- Security rights;
- Data protection impact assessment and prior consultation;
- Communicating data breach to data subject;
- Data Protection Officer;
- Remedies, liability and sanctions

that Facebook in Dublin is responsible for Facebook privacy and data protection in Europe and elsewhere (apart from the US and Canada). This position is not universal with other multinationals, however.

Section 15 of the DPA 1998 refers to jurisdiction and procedure. Section 15(1) provides that the jurisdiction conferred by ss 7 to 14 is exercisable by the High Court or a county court or, in Scotland, by the Court of Session or the sheriff. Section 15(2) provides that for the purpose of determining any question whether an *applicant under* sub-s (9) of s 7 is entitled to the information which he seeks (including any question whether any relevant data are exempt from that section by virtue of Part IV) a court may require the information constituting any data processed by or on behalf of the Controller and any information as to the logic involved in any decision-making as mentioned in s 7(l)(d) to be made available for its own inspection but shall not, pending the determination of that question in the applicant's favour, require the information sought by the applicant to be disclosed to them or his representative weather by the discovery (or in Scotland, recovery) or otherwise. Certain internet companies, however, seek to avoid liability to the UK and EU data protection regimes by segregating services and seeking to suggest that the entire service and surrounding infrastructure is located outside of the UK and EU. These are ongoing issues of contention.

GDPR Recital 22 states that any processing of personal data in the context of the activities of an establishment of a Controller or a Processor in the EU should be carried out in accordance with the Regulation, regardless of whether the processing itself takes place within the EU. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.

GDPR Recital 23 states that in order to ensure that natural persons are not deprived of the protection to which they are entitled under the GDPR, the processing of personal data of Data Subjects who are in the EU by a Controller or a Processor not established in the EU should be subject to the GDPR where the processing activities are related to the offering of goods or services to such Data Subjects irrespective of whether connected to a payment.

Recital 36 states that the main establishment of a Controller in the EU should be the place of its central administration in the EU unless the decisions on the purposes

and means of the processing of personal data are taken in another establishment of the Controller in the EU, in which case that other establishment should be considered to be the main establishment. Further details such as objective criteria are also referred to.

Third country Controllers must appoint a Representative in EU. GDPR Recital 80 states that where a Controller not established in the EU is processing personal data of Data Subjects residing in the EU whose processing activities are related to the offering of goods or services to such Data Subjects, or to the monitoring their behaviour, the Controller should designate a representative.

It is also noted that there is no exception made in the GDPR for UGC or user generated content.

Article 3 of the GDPR provides that the GDPR applies to the processing of personal data in the context of the activities of an establishment of a Controller or a Processor in the EU, regardless of whether the processing takes place in the EU or not.

The GDPR applies to the processing of personal data of Data Subjects who are in the EU by a Controller or Processor not established in the EU, where the processing activities are related to,

- the offering of goods or services, irrespective of whether payment of the Data Subject is required, to such Data Subjects in the EU; or
- the monitoring of their behaviour as far as their behaviour takes place within the EU.

The GDPR applies to the processing of personal data by a Controller not established in the EU, but in a place where Member State applies by virtue of public international law.

## 4.6 INVESTIGATIONS OF SOCIAL MEDIA ORGANIZATIONS

Social Media organizations can be officially investigated and audited much like any other organizations can.[47]

Perhaps in terms of social media, one of the most useful resources available to those interested in understanding how sites may be regulated was its audit. Facebook

[47] Facebook Ireland Limited Report of re-audit: Data Protection Commissioner, 21 September 2012. *available at:* http://edepositireland.ie/handle/2262/81672 (last visited on May 30, 2022).

was audited by the Irish Data Protection Commissioner[48] as a result of a number of complaints raised by data subjects concerning the protection of their data on the site. Facebook in Europe is based in Ireland, which is why the audit was conducted by the Irish regulator.

In December 2011, the Commissioner published the results of a detailed audit of Facebook. The 2012 report summarized the outcome of that review in terms of the following areas, which were highlighted as being of concern from a data protection perspective.

Privacy policies; Advertising; Access requests retention; Cookies and plug-ins; Third-party apps; Disclosure of content to third parties; Facial recognition and tags; Data security; Deletion of accounts; Friend finders; Posting on other users' and groups' profile pages; Facebook credits; Profiles of individuals using the site under an alias name; Reporting abusive content and behaviours; Compliance systems put in place by the site; Site governance.

The list detailed above and the content of the report was by no means an exhaustive restatement of all of the issues raised in relation to social networking sites and privacy concerns. Clearly, as the site develops increasingly sophisticated platform developments, new concerns may arise. In respect of the site, as it was in 2012, a number of complaints have been raised by pressure groups, such as *Europe Against Facebook,* which is still outstanding.[49]

The investigation into the operation of the site has meant that Facebook has had to make a number of changes to the site in order to comply with the privacy principles brought to its attention by the Irish Commissioner. Significantly, the controversial site feature of face recognition has had to be turned off for users in the EU (Facebook Ireland is responsible for all Facebook activities outside of the USA and Canada). Users must also now be given the right to delete their accounts, in order to comply with the fifth principle that data must not be kept for longer than is necessary.

The UK *Leveson Report* deals with (certain) data protection issues in detail, namely the recommendations relating to data protection and journalism.[50] Amongst the

[48] Facebook Ireland Limited Report of re-audit: Data Protection Commissioner, 21 September 2012. *available at:* http://edepositireland.ie/handle/2262/81672 (last visited on May 30, 2022).
[49] htttp://www.europe-v-facebook.org/EN/en/html.
[50] *Supra* note 9.

many witnesses at the *Leveson Inquiry* were Facebook, Google, and Twitter. One of the headline issues relates to what activities and services they engage in, respectively, and what they can and can't do in terms of specific content. These are controversial and evolving issues in terms of both data protection compliance as well as take downs and liability for the material on (and via) their websites.[51]

During the course of the Leveson Inquiry,[52] a number of website operators and micro site platforms were called to give evidence, most notably Twitter, Google, and Facebook. A number of questions were raised in relation to the activities of the sites.

Twitter in particular came into focus and was of interest to the Inquiry because of the role played by users in identifying individuals who had been the subject of privacy injunctions. Twitter allows members to operate anonymously, or under a pseudonym, and it is also possible that the company itself may not know the real identity of any member. However, Twitter told the Inquiry that its rules forbid members from using the service for any unlawful purpose, and any material that is found by the company to contravene that policy can be taken down or removed.[53]

## 4.7 PRIVACY LAWS IN SOME COUNTRIES

Most of the countries of the world have adopted legislations to protect the privacy of the individuals in social media platforms. A few of them are as follows:

### 4.7.1 GERMANY

Privacy in Germany is regulated by the *Federal Commissioner for Data Protection and Freedom of Information.* Germany has one of the strictest privacy policies in the world.

### 4.7.2 THE UNITED STATES

Privacy in the United States is found in a number of places that deal with contexts and dimensions of privacy. The main policy tools include the Privacy Act of 1997, the privacy provisions of the E-Governance Act of 2002, the Federal Information Security Management Act, and further policy directives that are created as an extension of these Acts. Certain privacy rights are being protected in the United States by

[51] *Ibid.*
[52] Lord Justice Leveson, *Report into the Culture Practices and Ethics of the Press,*29 November 2012. London: Department for Culture, Media and Sport. HC 8708-i-iii, 2012-13.
[53] *Supra* note 12.

specialized legislation such as the Children's Online Privacy Protection Act (COPRA), which gives parents control over what information websites can collect from their children. The California Online Privacy Protection Act (OPPA) demands a privacy policy from online services companies that collect personal data from its residents to publish on their websites. This is particularly important, taking into consideration that Facebook and other major online companies are headquartered in California.[54] However, the California Office of the Information Security and Privacy Protection adopts a more relaxed approach to what private companies are allowed to do within their privacy policies.

### 4.7.3 CANADA

Canada has taken a leading international role in investigating privacy violations in the context of Facebook, and its approach is closer to the European model. The office of the Privacy Commissioner of Canada (OPC) was created in 1997 to protect Canadian consumers' privacy rights. One of the policy tools is the Personal Information Protection and Electronic Documents Act (PIPEDA) 2000.

## 4.8 HUMAN RIGHTS LAW AND PRIVATE ACTORS

Human rights law is state-centric in nature in the sense that states - not individuals, not companies - are the primary duty bearers. Legally speaking, only the state can be brought before a human rights court, such as the European Court of Human Rights, and examined for alleged human rights violations. Part of this obligation, however, is a duty upon the state to ensure that private actors do not violate human rights, referred to as the horizontal effect of human rights law. National regulation related to labour rights or data protection, for example, serves as machinery for enforcing human rights standards in the realm of private parties.[55]

Whereas human rights law is focused on the vertical relation (state obligations to the individual), it recognizes the horizontal effect that may arise in the sphere between private parties. The horizontal effect implies a state duty to protect human rights in the realm of private parties, for example, via industry regulation.[56]

[54] *Supra* note 10 at 478.
[55] Molly K. Land and Jay D. Aronson (eds), *New Technologies for Human Rights Law and Practice* 253 (Cambridge University Press, New Delhi, 2018).
[56] *Ibid.*

Over the past decade, the interface between human rights law and private actors has been the focus of considerable attention, resulting in the adoption of broad soft law standards and the launch of many multistakeholder initiatives, including the UN Global Compact. The UN Global Compact represents one of the core platforms for promoting corporate social responsibility (CSR), a concept that refers to a company's efforts to integrate social and environmental concerns into its business operations and stakeholder interactions. According to the UN Global Compact's framing of corporate social responsibility, businesses are responsible for human rights within their sphere of influence. While the sphere of influence concept is not defined in detail by international human rights standards, it tends to include the individuals to whom a company has a certain political, contractual, economic, or geographic proximity. Arguably, CSR has some normative base in the human rights discourse, but these rights have not been well integrated.[57]

### 4.8.1 RUGGIE'S "PROTECT, RESPECT AND REMEDY" FRAMEWORK

In 2011, Ruggies work culminated with an endorsement of the United Nations' Guiding Principles on Business and Human Rights (UNGP).[58] The UNGP provides a set of principles that states and businesses should apply to prevent, mitigate, and redress corporate related human rights abuses. Contrary to the sphere of influence approach, the UNGP focuses on the potential and actual human rights impact of any business conduct. The UNGP elaborates on the distinction that exists between the state duty to protect human rights and the corporate responsibility to respect human rights based on three pillars, often called the "Protect, Respect, and Remedy" framework. The first pillar (Protect) focuses on the role of the state in protecting individuals' human rights against abuses committed by non-state actors; the second pillar (Respect) addresses the corporate responsibility to respect human rights, and the third pillar (Remedy) explores the roles of state and non-state actors in securing access to remedy.[59] Ruggie's report to the Human Rights Council, which provided the basis for the UNGP, explains:

[57] *Ibid.*
[58] UN General Assembly, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework,* UN Doc. A/HRC/17/31 (March 21, 2011). *available at*:
https://documents-dds-ny.un.org/doc/UNDOC/GEN/G11/121/90/PDF/G1112190.pdf?OpenElement (last visited on May 30, 2022).
[59] Supra note 55 at 255.

> *"Each pillar is an essential component in an inter-related and dynamic system of preventative and remedial measures: the State duty to protect because it lies at the very core of the international human rights regime; the corporate responsibility to respect because it is the basic expectation society has of business in relation to human rights, and access to remedy because even the most concerted efforts cannot prevent all abuse".*[60]

The second pillar affords a central role for human rights due diligence by companies. Due diligence comprises four steps, taking the form of a continuous improvement cycle. Companies must publish a policy commitment to respect human rights. As part of due diligence process, a company must assess, using a human rights impact assessment, the actual and potential impacts of its business activities on human rights; remediate the findings of this assessment into company policies and practices; track how effective company is in preventing adverse human rights impacts; and communicate publicly about the due diligence process and its results.[61]

Whereas pillars one and three combine existing state obligations under international human rights law with soft law recommendations, pillar two is soft law only, reflecting the lack of direct human rights obligations for companies under international law. The debate on whether and how to create binding human rights obligations for companies has been ongoing for more than two decades, but there is little indication that companies will be bound by human rights law in the foreseeable future.[62]

It is well established in human rights law that private entities are also equally responsible for protecting human rights and freedoms against unlawful interference by State and non-State actors. Companies should adhere to the "Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and

[60] UN General Assembly, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework,* UN Doc. A/HRC/17/31 (March 21, 2011). *available at*: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G11/121/90/PDF/G1112190.pdf?OpenElement (last visited on May 30, 2022).
[61] UN General Assembly, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework,* UN Doc. A/HRC/17/31 p. 24 (March 21, 2011). *available at*: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G11/121/90/PDF/G1112190.pdf?OpenElement (last visited on May 30, 2022).
[62] *Supra* note 55 at 256.

Remedy' Framework"[63], the Global Network Initiative's Principles on Freedom of Expression and Privacy,[64] the European Commission's ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights,[65] and the Telecommunications Industry Dialogue Guiding Principles. Companies, like States, should refrain from blocking or limiting the transmission of encrypted communications and permit anonymous communication. Corporate actors that supply technology to undermine encryption and anonymity should be especially transparent as to their products and customers. The use of encryption and anonymity tools and better digital literacy should be encouraged.[66]

### 4.8.2 LEGALITY, NECESSITY, AND PROPORTIONALITY TEST

Human rights law is implicated when a state interferes with the right to privacy, which occurs when the contents of communications or communications data are collected by state authorities, regardless of whether the data is examined. Once authorities examine data that has been collected, a second interference takes place. Retaining data over time interferes with the right to privacy, as does sharing communications data with other parties. Restricting anonymity in digital communications is also, considered to be an interference with the right to privacy, because anonymous and secure communications allow the free exchange of information and ideas, and anonymity "may be the only way in which many can explore basic aspects of identity, such as one's gender, religion, ethnicity, national origin or sexuality.[67]

---

[63] UN General Assembly, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework,* UN Doc. A/HRC/17/31 p. 24 (March 21, 2011). *available at*: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G11/121/90/PDF/G1112190.pdf?OpenElement (last visited on May 30, 2022).

[64] GNI PRINCIPLES ON FREEDOM OF EXPRESSION AND PRIVACY *available at*: https://globalnetworkinitiative.org/wp-content/uploads/2018/04/GNI-Principles-on-Freedom-of-Expression-and-Privacy.pdf (last visited on May 30, 2022).

[65] ICT sector guide on implementing the UN guiding principles on business and human rights, *available at:* https://op.europa.eu/en/publication-detail/-/publication/ab151420-d60a-40a7-b264-adce304e138b (last visited on May 30, 2022).

[66] UN General Assembly, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*, UN Doc. A/HRC/29/32 (May 22, 2015). *available at*: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A_HRC_29_32_en.doc (last visited on May 30, 2022).

[67] Molly K. Land and Jay D. Aronson (eds), *New Technologies for Human Rights Law and Practice* 225 (Cambridge University Press, New Delhi, 2018).

In order to be consistent with international human rights law, an interference with a qualified right such as privacy must meet the tests of legality, necessity, and proportionality. In terms of legality, the action constituting the interference (such as interception of communications) must be previously established in a law that is publicly accessible, clear, and precise, meaning that its consequences are foreseeable. Interference must be in pursuit of a legitimate aim, and it must be a necessary and proportionate means of achieving that aim. For the European Court of Human Rights, the measure must be "necessary in a democratic society," meaning that it must answer a "pressing social need," and state authorities must provide "relevant and sufficient" justifications for the measure.[68]

The court has established that states have a margin of appreciation in determining whether a measure is necessary and proportionate, particularly when the protection of national security is concerned. When a state engages in secret surveillance, the analysis focuses on whether the measures are "strictly necessary for safeguarding the democratic institutions" and whether "adequate and effective guarantees against abuse" are in place.[69]

For the European Court, laws containing a great degree of specificity are more likely to be deemed consistent with the European Convention. The law should specify the nature of the offenses for which surveillance can be ordered, which individuals' communications can be monitored, and which authorities are empowered to request, order, and carry out surveillance, as well as the procedure to be followed. It should provide for "a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the (circumstances in which recordings may or must be erased or destroyed."[70]

For years, human rights bodies have emphasized that although advances in communications technology require an evolution in legal safeguards, the tests of legality, necessity, and proportionality continue to apply.[71]

[68] *Supra* note 55 at 225.
[69] *Ibid.*
[70] *Supra* note 55 at 226.
[71] *Supra* note 55 at 227.

## 4.9 UNITED NATION'S ROLE IN THE PROTECTION OF PRIVACY

The first UN instrument dealing directly with data privacy matters was a 1968 resolution of the General Assembly inviting the UN Secretary-General to examine, inter alia, individuals' right to privacy 'in the light of advances in recording and other techniques'. The resulting study by the Secretary-General led to the publication of a report in 1976 urging states to adopt data privacy legislation covering computerized personal data systems in the public and private sectors, and listing minimum standards for such legislation.[72]

In 1990, the UN General Assembly adopted a set of Guidelines on data privacy which repeat and strengthen this call.[73] Work on the Guidelines was rooted primarily in human rights concerns; was rooted primarily in human rights concerns; commercial anxieties about restrictions on transborder data flows appear to have taken a back seat. The adoption of the Guidelines underlined at the time that data privacy had ceased to be exclusively a 'first world', Western concern.[74]

In the further section the researcher analyses different resolutions adopted by UN General Assembly and Human Right Council's reports' on "the right to privacy in the digital age" since the first resolution in 2013[75] and its trends with changing technologies like social media, Big Data, Artificial Intelligence. The researcher further discusses recommendations made by the UN to be implemented by states and business enterprises.

### 4.9.1 MASS SURVEILLANCE AND VIOLATION OF PRIVACY

Since the Snowden revelations of mass surveillance in 2013, the United Nations (U.N.) General Assembly and U.N. Human Rights Council have considered resolutions

[72] Lee A. Bygrave, *Data Privacy Law An International Perspective* 51 (Oxford University Press, United Kingdom, 2014).
[73] UN General Assembly, *Guidelines Concerning Computerized Personal Data Files,* GA Res 45/95, GAOR, UN Doc E/CN4/1990/72 (December 14, 1990).
[74] *Supra* note 72.
[75] UN General Assembly, *The right to privacy in the digital age,* GA Res 68/167, GAOR, UN Doc A/RES/68/167 (December 18, 2013). *available at*: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/449/47/PDF/N1344947.pdf?OpenElement (last visited on May 30, 2022).

on "the right to privacy in the digital age" every year, each taking turns to pass the text biennially.[76]

From time to time UN adopted resolutions on the right to privacy in the digital age. UN through their resolutions *inter alia* General Assembly resolutions 68/167 of 2013[77], 69/166 of 2014[78], 71/199 of 2016[79] and 73/179 of 2018[80] on the right to privacy in the digital age, and resolution 45/95 of 1990[81] on guidelines for the regulation of computerized personal data files, as well as Human Rights Council resolutions 28/16 of 2015[82], 34/7 of 2017[83],6 37/2 of 2018[84] and 42/15 of 2019[85] on the right to privacy

[76] UN: To protect privacy in the digital age, world governments can and must do more, *available at:* https://www.article19.org/resources/un-to-protect-privacy-in-the-digital-age-world-governments-can-and-must-do-more/ (last visited on May 30, 2022).

[77] UN General Assembly, *The right to privacy in the digital age,* GA Res 68/167, GAOR, UN Doc A/RES/68/167 (December 18, 2013). *available at*: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/449/47/PDF/N1344947.pdf?OpenElement (last visited on May 30, 2022).

[78] UN General Assembly, *The right to privacy in the digital age,* GA Res 69/1667, GAOR, UN Doc A/RES/69/166 (February 10, 2015). a*vailable at:* https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/707/03/PDF/N1470703.pdf?OpenElement (last visited on May 30, 2022).

[79] UN General Assembly, *The right to privacy in the digital age,* GA Res 71/199 GAOR, UN DOC A/RES/71/199 (December 19, 2016). a*vailable at:* https://documents-dds-ny.un.org/doc/UNDOC/GEN/N16/455/32/PDF/N1645532.pdf?OpenElement (last visited on May 30, 2022).

80 UN General Assembly, The right to privacy in the dig*ital age,* GA Res 73/179, GAOR, UN Doc A/RES/73/179 (December 17, 2018). a*vailable at:* https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/449/97/PDF/N1844997.pdf?OpenElement (last visited on May 30, 2022).

**[81]** UN General Assembly, *Guidelines Concerning Computerized Personal Data Files,* GA Res 45/95, GAOR, UN Doc E/CN4/1990/72 (December 14, 1990).

[82] UN General Assembly, *The right to privacy in the digital age*, GA Res 28/16, GAOR, UN Doc A/HRC/RES/28/16 (April 1, 2015). *available at*: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/068/78/PDF/G1506878.pdf?OpenElement (last visited on May 30, 2022).

[83] UN General Assembly, *The right to privacy in the digital age*, GA Res 34/7, GAOR, UN Doc A/HRC/RES/34/7 (March 23, 2017). *available at:* https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/086/31/PDF/G1708631.pdf?OpenElement (last visited on May 30, 2022).

[84] UN General Assembly, *The right to privacy in the digital age*, GA Res 37/2, GAOR, UN Doc A/HRC/RES/37/2 (March 22, 2018). *available at:* https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/099/87/PDF/G1809987.pdf?OpenElement (last visited on May 30, 2022).

[85] UN General Assembly, Human Right Council, *The right to privacy in the digital age*, GA HRC Res 42/15, GAOR, UN Doc A/HRC/RES/42/15 (September 26, 2019). *available at:* https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/297/52/PDF/G1929752.pdf?OpenElement (last visited on May 30, 2022).

in the digital age and resolutions 32/13 of 2016[86] and 38/7 of 2018[87] on the promotion, protection, and enjoyment of human rights on the Internet have emphasized to take appropriate actions by the state and corporates to protect the privacy of individuals in the digital age.

In 2014, Human Right Council noted that the rapid pace of technological development enables individuals all over the world to use new information and communications technology and at the same time enhances the capacity of governments, companies, and individuals to undertake surveillance, interception, and data collection, which may violate or abuse human rights, in particular the right to privacy, as set out in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights, and is, therefore, an issue of increasing concern.[88]

The report on 'The Right to Privacy in the Digital Age 2014," recommended that States should review their own national laws, policies, and practices to ensure full conformity with international human rights law. A clear, precise, accessible, comprehensive, and non-discriminatory legislative framework is required in every State. An effective remedy should be provided to the victims.[89]

Considering the significance of privacy rights under the Human Rights law, the United Nations reported that the government's surveillance program should be limited. Every State must apply the data privacy principles while conducting its digital surveillance programs. Surveillance laws or programs should be publicly accessible; contain provisions for the collection of, access to and use of communications data should be used for specific legitimate purposes; are sufficiently precise, specifying in detail the precise circumstances in which any such interference may be permitted, the

[86] UN General Assembly, *The promotion, protection and enjoyment of human rights on the Internet,* GA Res 32/13, GAOR, UN Doc A/HRC/RES/32/13 (July 1, 2016). a*vailable at:* https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/156/90/PDF/G1615690.pdf?OpenElement (last visited on May 30, 2022).

[87] UN General Assembly, *The promotion, protection and enjoyment of human rights on the Internet,* GA Res 38/7, GAOR, UN Doc A/HRC/RES/38/7 (July 5 2018). a*vailable at*: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/215/67/PDF/G1821567.pdf?OpenElement (last visited on May 30, 2022).

[88] UN General Assembly*, The right to privacy in the digital age,* GA Res 27/37, GAOR, UN Doc A/HRC/27/37 (June 30, 2014). *available at*: http://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc (last visited on May 30, 2022).

89 UN General Assembly, The right to privacy in the digital age, GA Res 27/37, GAOR, UN Doc A/HRC/27/37 (June 30, 2014). available at: http://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc (last visited on May 30, 2022).

procedures for authorizing, the categories of persons who may be placed under surveillance, the limits on the duration of surveillance, and procedures for the use and storage of the data collected; and provide for effective safeguards against abuse.[90]

Increasingly, the United Nations requires that the State's interference into an individual's private life has to fulfill the 'quality of law' requirement that imposes three conditions namely the measure must have some basis in domestic law; the domestic law itself must be compatible with the rule of law and the requirements of the Covenant; and the relevant provisions of domestic law must be accessible, clear and precise. In other words, it means that the member States are supposed to make domestic law on surveillance that should be compatible with the principles of accessibility, specificity, foreseeability, standards of necessity and proportionality. The United Nations reported that the surveillance is allowed only if relevant States are in a position to justify as proportionate the systematic interference with the Internet privacy rights of a potentially unlimited number of innocent people located in any part of the world. Furthermore, it has been recommended that the victims should have the right to seek an effective remedy for any alleged violation of their online privacy rights. For this, an independent and impartial mechanism is required. The report concluded that the States are legally obliged to afford the same privacy protection for nationals and non-nationals and for those within and outside their jurisdiction. Asymmetrical privacy protection regimes are a clear violation of the requirements of the Covenant.

General Assembly emphasized that business enterprises have a responsibility to respect human rights as set out in the Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework.

### 4.9.2 PROTECTION OF METADATA

The human right council in its Twenty-eighth session held in March 2015, noted that "while metadata[91] can provide benefits, certain types of metadata, when aggregated, can reveal personal information and can give an insight into an individual's behaviour, social relationships, private preferences, and identity", therefore, it was emphasized that "States should respect international human rights obligations regarding

90 UN General Assembly, The right to privacy in the digital age, GA Res 27/37, GAOR, UN Doc A/HRC/27/37 (June 30, 2014). available at: http://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc (last visited on May 30, 2022).

91 Metadata is a set of data that describes and gives information about other data.

the right to privacy when they intercept digital communications of individuals and/or collect personal data from third parties, including private companies". The council recalled that business enterprises have a responsibility to respect human rights as set out in the Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework. The council showed its deep concern at the negative impact of that mass surveillance may have on the exercise and enjoyment of human rights.[92]

### 4.9.3 STATES TO PROMOTE AN APPROPRIATE ICT ENVIRONMENT

On 19 December 2016, General Assembly in its resolution no. 71/199[93] noted that "violations and abuses of the right to privacy in the digital age may affect all individuals, including with particular effects on women, as well as children and those who are vulnerable or marginalized" and "the increasing capabilities of business enterprises to collect, process and use personal data can pose a risk to the enjoyment of the right to privacy in the digital age".

Therefore, UN "Encourages all States to promote an open, secure, stable, accessible and peaceful information and communications technology environment based on respect for international law, including the obligations enshrined in the Charter of the United Nations and human rights instruments" and recalls that business enterprises have a responsibility to respect human rights, applicable laws, international principles, and standards.

Human Right Council on July 1, 2016 "Calls upon all States to address security concerns on the Internet in accordance with their international human rights obligations to ensure the protection of freedom of expression, freedom of association, privacy and other human rights online, including through national democratic, transparent institutions, based on the rule of law, in a way that ensures freedom and security on the

[92]UN General Assembly, *The right to privacy in the digital age,* GA Agenda item 3 UN DOC A/HRC/28/L.27 (March 24, 2015). a*vailable at:* https://documents-dds-ny.un.org/doc/UNDOC/LTD/G15/061/64/PDF/G1506164.pdf?OpenElement (last visited on May 30, 2022).

[93] UN General Assembly, *The right to privacy in the digital age,* GA Res 71/199 GAOR, UN DOC A/RES/71/199 (December 19, 2016). a*vailable at:* https://documents-dds-ny.un.org/doc/UNDOC/GEN/N16/455/32/PDF/N1645532.pdf?OpenElement (last visited on May 30, 2022).

Internet so that it can continue to be a vibrant force that generates economic, social and cultural development".[94]

### 4.9.4 ASSOCIATION OF RIGHT TO PRIVACY WITH OTHER RIGHTS

Human Right Council on March 23, 2017, in its resolution no. 34/7 recognized that "the right to privacy can enable the enjoyment of other rights and the free development of an individual's personality and identity, and an individual's ability to participate in political, economic, social and cultural life, and noting with concern that violations or abuses of the right to privacy might affect the enjoyment of other human rights, including the right to freedom of expression and to hold opinions without interference, and the right to freedom of peaceful assembly and association."

The council further shows it concerns that "automatic processing of personal data for individual profiling may lead to discrimination or decisions that otherwise have the potential to affect the enjoyment of human rights, including economic, social and cultural rights, and recognizing the need to further discuss and analyse these practices on the basis of international human rights law" and council recalls that "States should ensure that any interference with the right to privacy is consistent with the principles of legality, necessity, and proportionality."

### 4.9.5 DATA-DRIVEN TECHNOLOGIES TO BE MANAGED WITH GREAT CARE

On August 3, 2018, Human Rights Council submitted its report on the right to privacy in the digital age. Although data-driven technologies are beneficial, these technologies carry significant risks to an individual's privacy, human dignity, and autonomy if not managed with great care. The council observed that the exploitative nature of digital technologies affects the social, cultural, economic, and political fabric of modern societies. Increasingly powerful data-intensive technologies, such as big data and artificial intelligence, threaten to create an intrusive digital environment in which both States and business enterprises are able to conduct surveillance, analyse, predict and even manipulate people's behaviour to an unprecedented degree. United Nations

94 UN General Assembly, Human Right Council, The promotion, protection and enjoyment of human rights on the Internet, GA HRC Res 32/13, GAOR, UN Doc A/HRC/RES/32/13 (July 1, 2016). available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/156/90/PDF/G1615690.pdf?OpenElement (last visited on May 30, 2022).

High Commissioner for Human Rights recommended that the States should recognize the implications of the data-driven technologies; make comprehensive privacy legislation complying the international human rights law including the principles of legality, legitimate aim, necessity, and proportionality; ensure that the collection and retention of the biometric data is proportionate to achieve a legitimate aim; ensure that surveillance measures require reasonable suspicion that a particular individual has committed or is committing a criminal offence or is engaged in acts amounting to a specific threat to national security; constitute an independent body to monitor its data privacy practices; stop blanket, indiscriminate retention of communications data on telecommunications and other companies. The United Nations High Commissioner also recommended that business enterprises should bring transparency, accountability, security and confidentiality in their systems to protect the individuals' right to privacy in the digital space.[95]

[95] Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General, *The right to privacy in the digital age*, Human Rights Council, Thirty-ninth session, Agenda items 2 and 3, A/HRC/39/29 (3 August 3, 2018). *available at*:
https://www.ohchr.org/sites/default/files/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/A_HRC_39_29_EN.pdf (last visited on May 30, 2022).
Following are the recommendations:

- "Recognize the full implications of new technologies, in particular data driven technologies for the right to privacy but also for all other human rights";
- "Adopt strong, robust and comprehensive privacy legislation, including on data privacy, that complies with international human rights law";
- Ensure that data-intensive systems, including those involving the collection and retention of biometric data, are only deployed when States is in position to demonstrate that they are necessary and proportionate to achieve a legitimate aim;
- Establish independent authorities empowered to monitor State and private sector data privacy practices, investigate abuses, receive complaints from individuals and organizations, and have provisions of fines and other effective penalties for the unlawful processing of personal data by private and public bodies; complies with international human rights law, including the principles of legality, legitimate aim, necessity and proportionality;
- "Strengthen mechanisms for the independent authorization and oversight of State surveillance and ensure that those mechanisms are competent and adequately resourced to monitor and enforce the legality, necessity and proportionality of surveillance measures";
- "Review laws to ensure that they do not impose requirements of blanket, indiscriminate retention of communications data on telecommunications and other companies";
- Take steps in order to enhance transparency and accountability in the acquisition of surveillance technologies by States;
- "Fully implement their duty to protect against abuses of the right to privacy by business enterprises in all relevant sectors, including the ICT sector, by taking appropriate steps to prevent, investigate, punish and redress such abuse through effective policies, legislation, regulations and adjudication";
- "Ensure that all victims of violations and abuses of the right to privacy have access to effective remedies, including in cross-border cases".

### 4.9.6 ARTIFICIAL INTELLIGENCE (AI) AND THE RIGHT TO PRIVACY

On September 26, 2019 the Human Right Council in its resolution "noted that the use of artificial intelligence can contribute to the promotion and protection of human rights, and can also have far-reaching and global implications, including with regard to the right to privacy, that are transforming Governments and societies, economic sectors and the world of work" and council recognized that "despite its positive effects, the use of artificial intelligence that requires the processing of large amounts of data, often relating to personal data, including on an individual's behaviour, social relationships, private preferences, and identity, can pose serious risks to the right to privacy, in particular when employed for identification, tracking, profiling, facial recognition, behavioural prediction or the scoring of individuals".[96]

The council further recognized "the need for Governments, the private sector, international organizations, civil society, the technical and academic communities and all relevant stakeholders to be cognizant of the impact, opportunities and challenges of rapid technological change on the promotion and protection of human rights, as well as of its potential to facilitate efforts, to accelerate human progress and to promote and protect human rights and fundamental freedoms".

### 4.9.7 SOCIAL MEDIA AND THE RIGHT TO PRIVACY DURING COVID-19

UN General Assembly on 16 December, 2020 in its resolution 75/176 noted "the importance of protecting and respecting the right of individuals to privacy when designing, developing or deploying technological means in response to disasters, epidemics and pandemics, especially the coronavirus disease (COVID-19) pandemic, including digital exposure notification and contact tracing". [97]

UN General Assembly further shows it concerns "about the spread of disinformation and misinformation, particularly on social media platforms, which can be designed and implemented so as to mislead, to spread racism, xenophobia, negative stereotyping and stigmatization, to violate and abuse human rights, including the right

[96] UN General Assembly, *The right to privacy in the digital age*, GA Res 42/15, GAOR, UN Doc A/HRC/RES/42/15 (September 26, 2019). *available at:* https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/297/52/PDF/G1929752.pdf?OpenElement (last visited on May 30, 2022).

97 UN General Assembly, The right to privacy in the digital age, GA Res 75/176, GAOR, UN Doc A/RES/75/176 (December 16, 2020). available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N20/371/75/PDF/N2037175.pdf?OpenElement (last visited on May 30, 2022).

to privacy, to impede freedom of expression, including the freedom to seek, receive and impart information, and to incite all forms of violence, hatred, intolerance, discrimination and hostility, and emphasizing the important contribution of journalists, civil society and academia in countering this trend". Hence Assembly calls upon all states *inter alia* "to consider developing or maintaining and implementing legislation, regulations and policies to ensure that all business enterprises, including social media enterprises and other online platforms, fully respect the right to privacy and other relevant human rights in the design, development, deployment and evaluation of technologies, including artificial intelligence, and to provide individuals whose rights may have been violated or abused with access to an effective remedy, including compensation and guarantees of non-repetition".[98]

### 4.9.8 IMPACT OF AI ON THE RIGHT TO PRIVACY

The report[99] of the United Nations High Commissioner for Human Rights, mandated by the Human Rights Council in its resolution 42/15 highlighted that the widespread use of artificial intelligence, including profiling, automated decision-making and machine-learning technologies, by States and businesses affects the enjoyment of the right to privacy and associated rights.

Artificial Intelligence is used for managing information online by social media platforms to support content management systems. Social media companies use these systems to rank content and decide what to amplify and what to downgrade, including by personalizing these decisions to different individual users based on their profiles.

The present report highlights salient features of artificial intelligence (AI) technology and its impact on the right to privacy as follows:

(a) "The operation of AI systems can facilitate and deepen privacy intrusions and other interference with rights in a variety of ways".

[98] UN General Assembly, *The right to privacy in the digital age,* GA Res 75/176, GAOR, UN Doc A/RES/75/176 (December 16, 2020). a*vailable at:* https://documents-dds-ny.un.org/doc/UNDOC/GEN/N20/371/75/PDF/N2037175.pdf?OpenElement (last visited on May 30, 2022).

99 UN General Assembly, Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General The right to privacy in the digital age, UN Doc A/HRC/48/31 (September 13, 2021). available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/249/21/PDF/G2124921.pdf?OpenElement (last visited on May 30, 2022).

(b) "AI systems typically rely on large data sets, often including personal data. This incentivizes widespread data collection, storage and processing. Many businesses optimize services to collect as much data as possible. For example, online businesses like social media companies rely on the collection and monetization of massive amounts of data about Internet users".

(c) "Large data sets enable countless forms of analysis and sharing of data with third parties, often amounting to further privacy intrusions and incurring other adverse human rights impacts. Over time, the data can become inaccurate, irrelevant or carry over historic misidentification, thereby causing biased or erroneous outcomes of future data processing".

(d) "AI tools are widely used to seek insights into patterns of human behaviour. AI is also used to assess the likelihood of future behavior or events. AI-made inferences and predictions, despite their probabilistic nature, can be the basis for decisions affecting people's rights, at times in a fully automated way".

(e) "AI-based decisions are not free from error. Outputs from AI systems relying on faulty data can contribute to human rights violations in a multitude of ways, for example, by erroneously flagging an individual as a likely terrorist or as having committed welfare fraud".

### 4.9.9 UN RECOMMENDATIONS TO STATES AND BUSINESS ENTERPRISES

From time-to-time United Nations and its bodies since the inception of the first resolution in 2013 adopted on "the right to privacy in the digital age" rendered their recommendations to states and business enterprises to protect and respect the right to privacy of individuals and devise a mechanism to provide remedies to the injured parties. The researcher feels it pertinent to mention these recommendations[100] by the UN to states and business enterprises as follows:

**UN calls upon all States:**

(a) To respect and protect the right to privacy, including in the context of digital communications;

[100] These recommendations are based on General Assembly resolution 75/176 adopted on 16 December 2020, *available at* https://documents-dds-ny.un.org/doc/UNDOC/GEN/N20/371/75/PDF/N2037175.pdf?OpenElement (last visited on May 30, 2022).

(b) To take measures to put an end to violations of the right to privacy through enacting relevant national legislation which complies with their obligations under international human rights law;

(c) To review, on a regular basis, their procedures, practices, and legislation regarding the collection of personal data, as well as regarding the use of profiling, automated decision-making, machine learning, and biometric technologies, with a view to upholding the right to privacy;

(d) To establish or maintain existing independent, effective, adequately resourced, and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency and accountability for state surveillance of communications, their interception, and the collection of personal data;

(e) To provide an effective remedy to individuals whose right to privacy has been violated;

(f) To consider developing or maintaining and implementing adequate legislation, in consultation with business enterprises, international organizations, and civil society, with effective sanctions and appropriate remedies, that protects individuals against violations and abuses of the right to privacy, in case of unlawful and arbitrary collection, processing, retention, sharing or use of personal data by individuals, Governments, business enterprises and private organizations;

(g) To consider developing or maintaining and implementing legislation, regulations and policies to ensure that all business enterprises, including social media enterprises and other online platforms, fully respect the right to privacy and other relevant human rights in the design, development, deployment and evaluation of technologies, including artificial intelligence, and to provide individuals whose rights may have been violated or abused with access to an effective remedy, including compensation and guarantees of non-repetition;

(h) To consider adopting or maintaining data protection legislation, regulation and policies, in consonance with international human rights obligations, including the establishment of independent authorities with powers and resources to monitor data privacy practices, investigate violations and abuses and receive communications from individuals and organizations, and to provide appropriate remedies;

(i) To further develop or maintain, in this regard, preventive measures and remedies for violations and abuses of the right to privacy in the digital age that may affect all individuals, including where there are particular effects for women, as well as children;

(j) To provide effective and up-to-date guidance to business enterprises on how to respect human rights by advising on appropriate methods, including human rights due diligence;

(k) To promote quality education for all to foster, inter alia, digital literacy, and technical skills to effectively protect their privacy;

(l) To take steps to enable business enterprises to adopt adequate voluntary transparency measures with regard to requests by State authorities for access to private user data and information;

(m) To consider developing or maintaining legislation, preventive measures, and remedies addressing harm from the processing, use, sale or multiple resale or other corporate sharing of personal data without the individual's free, explicit, meaningful and informed consent;

(n) To take appropriate measures to ensure that digital or biometric identity programmes are designed, implemented, and operated in full compliance with the obligations of States under international human rights law;

**The resolution also calls upon all business enterprises that collect, store, use, share, and process data:**

(a) To respect human rights in accordance with the Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework[101], including the right to privacy in the digital age;

(b) To inform users in a clear and easily accessible way about the collection, use, sharing, and retention of their data that may affect their right to privacy and to establish transparency policies that allow for the free, informed, and meaningful consent of users, as appropriate;

[101] Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie *available at:* https://documents-dds-ny.un.org/doc/UNDOC/GEN/G11/121/90/PDF/G1112190.pdf?OpenElement (last visited on May 30, 2022).

(c) To implement administrative, technical and physical safeguards to ensure that data are processed lawfully and to ensure that such processing is limited to what is necessary in relation to the purposes of the processing and that the legitimacy of such purposes, as well as the accuracy, integrity, and confidentiality of the processing, is ensured;

(d) To ensure that respect for the right to privacy and other international human rights is incorporated into the design, operation, evaluation, and regulation of automated decision-making and machine-learning technologies and have a provision for compensation in case of human rights abuses;

(e) To ensure that individuals have access to their personal data and to adopt appropriate measures for the possibility to amend, correct, update, delete and withdraw consent for the data;

Resolution encourages business enterprises to work towards enabling technical solutions to secure and protect the confidentiality of digital communications, which may include measures for encryption, pseudonymization and anonymity, and calls upon States not to interfere with the use of such technical solutions, with any restrictions thereon complying with the obligations of States under international human rights law, and to enact policies that recognize and protect the privacy of individuals' digital communications.

## 4.10 CONCLUSION

The right to privacy has been recognized and accepted all over the world as an essential human right. Privacy is an important component of human personality. The right to privacy has been recognized across jurisdictions along with international and regional conventions. International human rights documents like article 12 of UDHR, article 17 of ICCPR, and many others deal with the right to privacy. In regional human rights conventions article 8 of ECHR, article 18 of ACHPR, and article 11 of ACHR are prominent which deal with the right to privacy.

Privacy and data protection are evolving in terms of how technology is changing how personal data are collected, used, and processed. The current data protection legal regime is perceived as requiring updating. There must be better awareness and more hands-on board management responsibility, planning, and data protection assessment, and including risk assessment, in advance of product or service launch via the Data

Protection by Design (DPbD) concept. There is explicit recognition of children under the data protection regime for the first time. Data protection compliance is now required to be much more considered, organized, and planned.

The intersection of data protection and social media is one of the most controversial issues in contemporary data protection practice. Users are concerned as to what personal data is being collected and what it will be used for. Naturally, social networks will seek to commercialize and use profile information for advertising and marketing purposes. This tension remains. Furthermore, the tension is elevated when the individuals using social media websites are children. Various tragic events create a new level of sensitivity and importance. While the GDPR is a welcome advancement, additional research is also needed, and on an ongoing basis.

The frequency of change in social media and new ways to collect and process new categories of personal data during social media activities means that the mechanics of complying with access requests will have to continually evolve. There is also an issue remaining with certain social networks currently as to whether they are fully or only partially / compliant in terms of responding to data access requests.

The debate on whether and how to create binding human rights obligations for companies has been ongoing for more than two decades, but there is little indication that companies will be bound by human rights law in the foreseeable future.

Ruggie's framework, which has been widely praised and endorsed by states as well as business enterprises, has also been criticized for its slow uptake, its ineffectiveness, and for not creating binding obligations on companies. Yet a hard-law punitive approach has also long had its skeptics, and numerous empirical studies have spoken to the significance of social factors, both internal and external in affecting companies' behavior.

# CHAPTER-V
# PRIVACY LAWS & SOCIAL MEDIA: INDIAN PERSPECTIVE

# CHAPTER V
# PRIVACY LAWS & SOCIAL MEDIA: INDIAN PERSPECTIVE

## 5.1 INTRODUCTION

Internet has opened up a new medium for exchange of information among users. Every second, millions of messages are being created, sent and accessed. We are living in an information driven world. Data has become an indispensable component of the internet and therefore, the economy. Some of the largest companies in the world have built business empires around the collection and processing of data. This massive pool of data collected by these companies allows them to invade the private lives of an individual, and in more cases than not, without the individual's consent. These companies have been able to escape from the consequences of these intrusions because of a principle that lies at the very foundation of the internet- self-regulation. Companies have gained knowledge about almost every aspect of an individual's life and the lack of viable alternative service providers forces consumers to stay with one service provider.

It is at this stage that State intervention becomes necessary to prevent the breach of the rights of its citizens. This intervention must be backed by a law. In the age of information, the state requires data for some legitimate purposes which would then make the state accountable for a fool proof data protection law. In the present chapter, the researcher discusses legal framework to protect privacy and data of citizens from state as well as non-state actors in India.

## 5.2 CONSTITUTIONAL BASIS FOR THE RIGHT TO PRIVACY IN INDIA

The right to privacy, before *Puttaswamy case*[1] derived its ambiguous basis from the right to life and personal liberty, as enshrined in Article 21. In the language of the over-arching Article of the Constitution of India, Article 21 reads as follows:

[1] *Justice (Retd.) K.S. Puttaswamy v. Union of India* (2017) 10 SCC 1.

**Article 21. Protection of life and Personal Liberty.** – *No person shall be deprived of his life and liberty except according to procedure established by law.*

In the period before the coming of the present Constitution, no rights were accorded to citizens. The legal concept of citizenship and enforceable rights in India came into being with the Constitution of 1950.

The province of privacy of an individual came to be determined by law. Criminal enactments afforded protections to the person, property and dwelling house and made it punishable to impute unchastity to a female. The law of torts provided an additional dimension of protection of individual interests in reputation as also the person and property with an admonition that the least touching of another in anger was assault actionable in damages. The right to reputation was exercised through the laws of libel and slander.[2]

In the first claim for a right to privacy the Supreme Court declined to impute a constitutional element of privacy in ***M.P. Sharma*** *v.* ***Satish Chandra***[3]**,** the Supreme Court 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 Supreme Court undertook a comprehensive examination of the question of the right to privacy in ***Kharak Singh***.[4] In the instant case, the question for consideration before the seven-judge Bench was whether surveillance under Chapter XX of the Uttar Pradesh Police Regulations infracted fundamental rights guaranteed by Part III of the Constitution. Regulation 236(6) which allowed surveillance by "domiciliary visits at night" was held to contravene Article 21. The court elaborately analysed the connotations of the words "life" and "personal liberty" in Article 21.

The majority opinion in the case ascribed enriched meaning to the terms "life" and personal liberty employed in Article 21:

*Is then the word 'personal liberty' to be construed as excluding from its purview an invasion on the part of the police of the sanctity of a man's home and an intrusion*

[2] Rishika Taneja and Sidhant Kumar, *Privacy Law Principles Injunctions and Compensation* 23 (Eastern Book Company, Lucknow, 2014).
[3] *M.P. Sharma v. Satish Chandra* AIR 1954 SC 300.
[4] *Kharak Singh v. State of Uttar Pradesh* (1964) I SCR 332.

*into his personal security and his right to sleep which is the normal comfort and a dire necessity for human existence even as an animal? It might not be inappropriate to refer here to the words of the preamble to the Constitution that it is designed to 'assure the dignity of the individual' and therefore of those cherished human values as the means of ensuring his full development and evolution. We are referring to these objectives of the framers merely to draw attention to the concepts underlying the constitution which would point to such vital words as 'personal liberty' having to the construed in a reasonable manner and to be attributed that sense which would promote and achieve those objectives and by no means to stretch the meaning of the phrase to square with any pre-conceived notions or doctrinaire constitutional theories.*

The minority opinion authored by Subba Rao J, however, went further to impute a right to privacy in clear terms as a component of "personal liberty":

*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; it is expected to give him rest, physical happiness, peace of mind and security.*

The minority view in the ***Kharak Singh case***[5] decision forms the foundation of the right to privacy as a fundamental right in the Indian constitutional system. It examines the scope and purport of such a right and its relevance to human dignity and personality. The subsequent pronouncements on the right to privacy derive their roots from this strident minority decision of Subba Rao J.

The Supreme Court in ***Gobind Case***[6], undertook a more comprehensive analysis of the right to privacy. The Court was considering the constitutionality of Regulations 855 and 856 of the Madhya Pradesh Police Regulations which provided for surveillance undertaken by various means specified therein including surveillance of habitual offenders through domiciliary visits and picketing. The Supreme Court upheld the validity of the regulations since it met the test of "procedure established by law" laid down in Article 21. The court also accepted a limited right to privacy rooted in Articles 19(1)(a), (d) and 21. The right, however, was not considered absolute in the court's view.

[5] *Kharak Singh v. State of Uttar Pradesh* (1964) I SCR 332.
[6] *Govind vs State Of Madhya Pradesh & Anr.* 1975 AIR 1378.

It was opined by the court that restrictions may be legitimately placed on the right in public interest in terms of Article 19(5).

Matthew J, envisaged the evolution of privacy right in a case-by-case development. In other words, it desisted from laying down overarching principles that would govern claims for privacy. The court was in favour of deciding such claims on the basis of the factual circumstances of each case. The court held as thus:

*The right to privacy will, therefore, necessarily, have to go through a process of case-by-case development. Hence, assuming that the right to personal liberty, the right to move freely throughout India, and the freedom of speech create an independent fundamental right of privacy as an emanation from them it could not be absolute. It must be subject to the restriction on the basis of compelling public interest. But the law infringing it must satisfy the compelling state interest test.*

The decision in the *Gobind case (supra)* therefore recognizes that there may be certain restrictions that may be placed on the right to privacy in the larger societal or public interest. Further, the Supreme Court accepts that such restrictions ought to be based on the compelling State interest test. It is our considered view that the test of restriction ought to conform to the dictum laid down by the Supreme Court in ***Maneka Gandhi* v. *Union of India***[7] and the balancing of these competing interests ought to be arrived at by a thorough process of balancing.

The Supreme Court in the ***Maneka Gandhi case (supra)*** held that the term "procedure established by law" employed in Article 21 is construed as a procedure that is "fair, just and reasonable" as opposed to being "arbitrary", "freakish" or bizarre.

The scope and ambit of the right of privacy came up for consideration before the Supreme Court in ***R. Rajagopal V. State of T. N.,***[8] popularly christened the "*Auto Shanker* Case" the Supreme Court has expressly held that the "right to privacy", or "the right to be let alone" is guaranteed by Article 21 of the Constitution. In the instant case, the alleged autobiography of Auto Shankar, who was convicted and sentenced to death for committing six murders, contained comments on his contact and personal relations with police officials. The court placed reliance on the seminal article by Warren and

[7] *Maneka Gandhi v. Union of India* (1978) 1 SCC 248.
[8] *R. Rajagopal v. State of T. N* (1994) 6 SCC 632.

Brandeis[9] which defined the concept of "the right to be left alone" while including within its ambit:

Hon'ble Supreme Court proposed certain canons upon which the definition of privacy may be based. These canons are:

(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 9(2)][10] 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.*

The Supreme Court recognises the need to limit the scope of privacy so as to prevent it from impacting transparency and legitimate freedom of expression. Therefore, comments made on matters in the public records are precluded from claims of privacy claims both in private and public law. However, the court does recognise the requirement of differential privacy protection is special circumstances such as cases of sexual violence.

(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*

[9] Samuel D. Warren & Louis D. Brandies, *The Right to Privacy,* 4 HARV. L. REV. 193 (1890).
[10] *District Registrar and Collector v. Canara Bank* (2005) I SCC 496: AIR 2005 SC 186.

*privacy, or for that matter, the remedy of action for damages is simply not available with respect 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.*

The decision of the Supreme court in the *Auto Shanker Case (supra)* forms the basis for privacy law in India. It recognizes privacy as a fundamental right protected by Article 21. This gives rise to public law remedies under Article 32 and 226 of the Constitution. However, the court goes further to recognize the breach of privacy as sound basis for a civil claim for damages and injunctions. Thereby, the roots for a private law action of privacy in Indian law were firmly established.

The Supreme Court after considering a number of authorities speaking through a two-judge Bench held in the landmark case of ***People's Union for Civil Liberties v. Union of India***[11] (PUCL):

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

The PUCL case arose from a petition in the public interest that was a response to revelations in the media that a large number of interceptions were being carried out

[11] (1997) I SCC 301: AIR 1997 SC 568.

by the State. The reports suggested that the telephones of prominent opposition figures were also being intercepted.

Another dimension has been added to the recognition of privacy rights, when in ***State v. Charulata Joshi***[12], the Supreme Court held that "the constitutional right to freedom of speech and expression conferred by Article 19 (1) (a) of the Constitution which includes the freedom of the press is not an absolute right. The press must first obtain the willingness of the person sought to be interviewed and no court can pass any order if the person to be interviewed expresses his unwillingness".

Further in ***Sharda v. Dharmpal***[13]**,** it was held by the Supreme Court that the right to privacy in terms of Article 21 of the Constitution is not an absolute right. If there were a conflict between the fundamental rights of two parties, that right which advances public morality would prevail.

In ***District Registrar and Collector v Canara Bank***[14]**,** it was held by the Supreme Court that:

*the exclusion of illegitimate intrusions into privacy depends on the nature of the right being asserted and the way in which it is brought into play, it is at this point that the context becomes crucial, to inform substantive judgment. If these factors are relevant for defining the right to privacy, they are quite relevant whenever there is invasion of that right by way of searches and seizures at the instance of the State.*

Similarly, in ***State of Maharashtra v. Madhukar Narayan Mardikar***[15], the Supreme Court protected the right to privacy of a prostitute. It was held that even a woman of easy virtue is entitled to her privacy and no one can invade her privacy as and when he likes.

Also, in ***Malak Singh v. State of Punjab and Haryana***[16]**,** wherein an application was filed by the applicants seeking to remove their names from the surveillance register maintained by the police station of their jurisdiction under the Punjab Police Rules. The Court while upholding the jurisdiction of Punjab Police made observations on the mode of surveillance and emphasised that surveillance must be conducted as per rules. However, in ***Bhavesh Jayanti Lakhani v State of Maharashtra***[17] the Court observed

[12] *State v. Charulata Joshi* (1999) 4 SCC 65.
[13] *Sharda v Dharmpal* (2003) 4 SCC 493.
[14] *District Registrar and Collector v. Canara Bank* (2005) 1 SCC 496.
[15] *State of Maharashtra v. Madhukar Narayan Mardikar* (1991) 1 SCC 57.
[16] *Malak Singh v. State of Punjab and Haryana* (1981) 1 SCC 420.
[17] *Bhavesh Jayanti Lakhani v. State of Maharashtra* (2010) 1SCC (Cri) 47.

that "no such guidelines, however, has been laid down in respect of surveillance conducted pursuant to a red corner or yellow corner notice (of Interpol). The Central Government and in particular the Ministry of External Affairs, in our opinion, should frame appropriate guidelines in this behalf". Further in ***Amar Singh v. UOI***[18]**,** the Hon'ble Supreme Court observed that "sanctity and regularity in official communication in such matters must be maintained especially when the service provider is taking the serious step of intercepting the telephone conversation of a person and by doing so is invading the privacy right of the person concerned which is a fundamental right protected under the Constitution, as has been held by this Court." In view of the public nature of the function of a service provider, it is inherent in its duty to act carefully and with a sense of responsibility.

In ***Ram Jethmalani v. UOI***[19] the Supreme Court has dealt with the right to privacy elaborately and held as under:

*The right to privacy is an integral part of the right to life. This is a cherished constitutional value, and it is important that human beings should be allowed domains of freedom that are free of public scrutiny unless they act in an unlawful manner...*

*The solution for the problem of abrogation of one zone of constitutional values cannot be the creation of another zone of abrogation of constitutional values... The notion of fundamental rights, such as a right to privacy as part of the 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.*

Privacy debate has taken a different turn when during the "Aadhaar case" hearings before the Supreme Court, the Union of India took a stand - whether privacy is a fundamental right, this needs to be examined by a larger Constitutional Bench as the previous judgments have failed to clear the confusion?

In this batch of matters, a scheme propounded by the Government of India popularly known as "Aadhaar Card Scheme" was under attack on various counts. It was alleged by the petitioners under the said scheme the Government of India was collecting and compiling both the demographic and biometric data of the residents of this country to be used for various purposes.

[18] *Amar Singh v. UOI* (2011) 7 SCC 69.
[19] *Ram Jethmalani v. UOI* (2011) 8 SCC 1.

One of the grounds of attack on the scheme was that the very collection of such biometric data is violative of the "right to privacy". Some of the petitioners asserted that the right to privacy is implied under Article 21 of the Constitution of India while other petitioners asserted that such a right emanates not only from Article 21 but also from various other articles embodying the fundamental rights guaranteed under Part-Ill of the Constitution of India.

Supreme Court in its order in ***Justice K.S. Puttaswamy (Retd.) v UOI***[20]**,** opined:

12. We are of the opinion that the cases on hand raise far reaching questions of importance involving interpretation of the Constitution. What is at stake is the amplitude of the fundamental rights including that precious and inalienable right under Article 21. If the observations made in *M.P Sharma (supra)* and *Kharak Singh (supra)* are to be read literally and accepted as the law of this country, the fundamental rights guaranteed under the Constitution of India and more particularly right to liberty under Article 21 would be denuded of vigour and vitality. At the same time, we are also of the opinion that the institutional integrity and judicial discipline require that pronouncement made by larger Benches of this Court cannot be ignored by the smaller Benches without appropriately explaining the reasons for not following the pronouncements made by such larger Benches. With due respect to all the learned Judges who rendered the subsequent judgments - where right to privacy is asserted or referred to their lordships concern for the liberty of human beings, we are of the humble opinion that these appears to be certain amount of apparent unresolved contradiction in the law declared by this Court.

13. Therefore, in our opinion to give a quietus to the kind of controversy raised in this batch of cases once for all, it is better that the *ratio decidendi* of *M.P. Sharma* (supra) and *Kharak Singh* (supra) is scrutinised and the jurisprudential correctness of the subsequent decisions of this Court where the right to privacy is either asserted or referred be examined and authoritatively decided by a Bench of appropriate strength.

14. We, therefore, direct the Registry to place these matters before the Hon'ble the Chief Justice of India for appropriate orders.

[20] *Justice K.S. Puttaswamy (Retd.) v. UOI*, Writ Petition No. 494 of 2012, decided on 25th August 2017.

## 5.3 RIGHT TO PRIVACY – PUTTASWAMY DECISION

On 24 August 2017, a Constitutional Bench of nine judges of the Supreme Court of India in ***Justice K.S. Puttaswamy (Retd.) v UOI*** *(supra)* upheld that Privacy is a Fundamental Right, which is entrenched in Article 21 [Right to Life & Liberty]. All the judges expressed their opinions on the subject (running into 574 pages), which are being crystalised herein below:

**1.** Privacy is one of the most important rights to be protected both against state and non-state actors (body corporates), however it is not an absolute right and is subject to certain reasonable restrictions, which the state is entitled to impose on the basis of social, moral and compelling public interest in accordance with the law.

**2.** Privacy is not just a common law right, but a fundamental right.

**3.** The right to privacy is claimed qua the state and non-state actors. Recognition and enforcement of claims qua non-state actors may require legislative intervention by the state.

**4.** A robust privacy regime to ensure fulfillment of a three-fold requirement. These three requirements apply to all restraints on privacy (not just informational privacy). **The first** requirement is that there must be a law in existence to justify an encroachment on privacy. **Second,** the requirement of a need, in terms of a legitimate state aim, ensures that the nature and content of the law which imposes the restriction falls within the zone of reasonableness, which is a guarantee against arbitrary state action. The pursuit of a legitimate state aim ensures that the law does not suffer from manifest arbitrariness. **The third** requirement ensures that the means which are adopted by the legislature are proportional to the object and needs sought to be fulfilled by the law. Proportionality is an essential facet of the guarantee against arbitrary state action because it ensures that the nature and quality of the encroachment on the right is not disproportionate to the purpose of the law. Hence, the three-fold requirement for a valid law arises out of the mutual inter-dependence between the fundamental guarantees against arbitrariness on the one hand and the protection of life and personal liberty, on the other.

**5.** The balance between data regulation and individual privacy raises complex issues requiring delicate balances to be drawn between the legitimate concerns of the state on one hand and individual interest in the protection of privacy on the other.

**6.** Privacy has both positive and negative content. The negative content restrains the state from committing an intrusion upon the life and personal liberty of a citizen. Its positive content imposes an obligation on the state to take all necessary measures to protect the privacy of the individual.

**7.** Restrictions of the right to privacy may be justifiable in the following circumstances subject to the principle of proportionality:

**(a)** Other fundamental rights: The right to privacy must he considered in relation to its function in society and be balanced against other fundamental rights

**(b)** Legitimate national security interest

**(c)** Public interest including scientific or historical research purposes or statistical purposes

**(d)** Criminal Offences: the need of the competent authorities for prevention investigation, prosecution of criminal offences including safeguards against threat to public security

**(e)** The unidentifiable data.

**8.** Data protection rules according to the objectives of the processing. There may however, be processing which is compatible for the purposes for which it is initially collected. The state must ensure that information is not used without the consent of users and that is used for the purpose and to the extent it was disclosed.

**9.** The Judgment has endorsed broadly the following principles: (a) Consent, (b) Choice, (c) Purpose, (d) Collection, (e) Disclosure, (f) Retention, (g) Proportionality and (h) legitimacy

## 5.4 LIABILITIES OF THE INTERMEDIARIES UNDER IT ACT, 2000

An intermediary represents nuts-and-bolts of an interactive network service. It may provide access to the Internet (network of networks) only or offer a range of additional resources or services. Depending upon its functional attributes an intermediary while performing the role of a network service provider may act as an 'information carrier' or 'information publisher'.

Intermediaries are being defined as under section 2(1)(w) of IT Act as: *"intermediary", with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record. The term network service provider is ever*

*expanding one. It is now being seen as synonymous with the term intermedial and includes telecom service providers, network service providers, Internet service providers, web-hosting service providers, search engines, online payment sites, online auction sites, online market places and cyber cafes.*

Intermediary may be broadly classified as 'information carriers', 'information publishers', or 'information sellers' depending on their functional attributes:

| **Information Carrier** | **Information Publisher** | **Information Seller** |
|---|---|---|
| Intermediary which merely acts as a carrier of information transmitting 'electronic message' from one place to another, without examining its content. Its primary role is to provide access to Internet connectivity to the users | Intermediary which publishes and transmits the information. | Intermediary, which publishes, transmits and sells the information/products and may take reasonable care in relations to its publication |
| *Examples:* 'Access only' intermediaries like, airtel.in, rcom.co.in, etc. google.com etc. | *Examples:* 'Enhanced' intermediaries like, yahoo.co.in, rediff.com. | *Examples:* 'E-commerce portals like ebay.in, Indiatimes.com, flipkart.com, amazon.in etc. |

**Table 5.1: Different Roles of Intermediary**[21]

Intermediaries are considered as spokes of the Internet wheel. Without these spokes, internet as a medium will simply collapse. Intermediaries represent technological innovation, which can be used in a lawful or unlawful manner. Hence, the idea is to balance the rights of intermediaries within the legal framework, without disturbing the benefits accruing to the society at large from technological innovations. In other words, regulation comes after understanding technology. It was thus felt by the lawmakers that any provision, which would limit the role of intermediaries might affect the growth of Internet - therefore a balance is needed. Section 79[22] of IT Act provides that balance between "technology necessity" and "legal necessity".

[21] Vakul Sharma and Seema Sharma, *Information Technology Law and Practices* 334 (Universal LexisNexis, India, 7th Edition, 2021).

[22] The Information Technology Act, 2000 (Act 21 of 2000) s. 79 read as - *Exemption from liability of intermediary in certain cases* - (I) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third-party information, data, or communication link made available or hosted by him.

Generally speaking, intermediaries being facilitator of third-party information, data, or communication link may be held liable for copyright infringement, trademark infringement/ dilution, privacy violations, obscenity, defamation, child pornography, spamming, etc. The offended parties may not only seek injunctions against such intermediaries to block/remove offending content, but may also initiate civil and criminal proceedings against them. For example, ***Gremach Infrastructure Equipments & Projects Ltd. V. Google India***[23] the Bombay High court held:

> *… prima facie***,** *at present stage, there is merit in the contention of the Plaintiffs that the article [Toxic Fumes] put up by the defendant on the blog site is defamatory... defendant to disclose particulars, names and the address of the person who is author of the article.*

Also, in ***YouTube LLC & Google Inc. v. Lebara Foundation***[24]**,** the Division Bench of the Madras High Court directed disclosure of identities of individuals who have posted *prima facie* offensive material. Similarly, there have been hundreds of cases [Civil Suits] in India, *wherein* various High Courts have issued ad-interim injunctions against the intermediaries, the list includes, ***Yugant Ram Marlapale v. UOI***[25] ***Mohit Kumar v. hh*.mohitkumar@gmail.com,**[26]***JCB India v. Abhinav***

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

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

[23] *Gremach Infrastructure Equipments & Projects Ltd. V. Google India,* Notice of Motion No. 668 of 2008 in Suit No. 506 of 2008, order dated 26 February 2008.

[24] *YouTube LLC & Google Inc. v. Lebara Foundation,* O.S.A. No. 213 of 2016, order dated 25 October 2016.

[25] *Yugant Ram Marlapale v UOI,* WP (Civil) 6554 of 2006, order dated 17 March 2008 (Aurangabad Bench of Bombay High Court). This was one of the earliest cases related to blocking on content on social media – Orkut. The Court ordered: "*we direct the Respondents No. 1 to 7 to keep vigil as to whether the objectional material by the impugned community is again displayed in future. The Petitioner is at liberty to occasionally test if the material from the impugned community is displayed on the Internet."*

[26] *Mohit Kumar v. hh.* mohitkumar@gmail.com*,* CS (OS) No. 1021 of 2008,. Order dated 24 May 2008.

***Gupta*[27], *JCB India v. IP Address 122.163.98.166*[28], *JCB India v. abhinavdeep@indiatimes.com*[29], *VMD CAD & Graphic Technologies v. Ambuj Kumar Goel*[30], etc.**

In ***Google India Pvt. Ltd. v. Visakha Industries*[31],** the issue before the Supreme Court was whether non-compliance with the notice to take down the defamatory posting on the Google platform is violative of section 79, which existed in the statute before its substitution in the Information Technology (Amendment) Act, 2008? Court held:

1. We reject the contention of the appellant that the High Court should have acted on the Google LLC conditions and found that the appellant is not the intermediary. We hold that this is a matter for trial.
2. We hold that Section 79 of the Act, prior to its substitution, did not protect an intermediary in regard to the offence under Section 499/500 of the IPC.
3. We set aside the findings by the High Court regarding the alleged refusal of the appellant to respond to the notice to remove. We make it clear, however, that it is for the Court to decide the matter on the basis of the materials placed before it, and taking into consideration, the observations contained in this judgment.

Section 79 does provide immunity but it is not absolute immunity. It clearly states that an intermediary shall not be liable for any third-party information, data or communication link made available or hosted by him. Under the IT Act, an intermediary in order to qualify for 'immunity' needs to observe Intermediary guidelines as notified by the Central Government.

### 5.4.1 INTERMEDIARY LIABILITY ARTICULATED IN SHREYA SINGHAL JUDGMENT

Supreme Court in its judgment Shreya Singhal v UOI[32] has opined:

*It must first be appreciated that section 79 is an exemption provision. Being an exemption provision, it if closely related to provisions which provide for offences including section 69A. We have seen how under section 69A blocking can take place*

---

[27] *JCB India v. Abhinav Gupta,* CS(OS) No. 691 of 2008, order dated 21 April 2008.
[28] *JCB India v. IP Address 122.163.98.166,* CS (OS) No. 1021 of 2008,. Order dated 24 May 2008.
[29] *JCB India v.* abhinavdeep@indiatimes.com*, CS (OS) No. 1143 of 2008 order dated 3 June 2008.*
*30 VMD CAD & Graphic Technologies v. Ambuj Kumar Goel,* CS (OS) No. 142 of 2009 order dated 23 January 2009.
[31] *Google India Pvt. Ltd. V. Visakha Industries,* Criminal Appeal No. 1987 of 2014, decided on 19 December 2019.
[32] *Shreya Singhal v. UOI,* AIR 2015 SC 1523.

*only by a reasoned order after comply with several procedural safeguards including a hearing to the originator and Intermediary. We have also seen how there are only two ways in which a blocking order can be passed - one by the Designated Officer after complying with the 2009 Rules and the other by the Designated Officer when he has to follow an order passed by a competent court. The intermediary applying its own mind to whether information should or should not be blocked is noticeably absent in section 61A read with 2009 Rules.*

*Section 79(3)(b) has to be read down to mean that the intermediary upon receiving actual knowledge that a court order has been passed asking it to expeditiously remove or disable access to certain material must then fall to expeditiously remove or disable access to that material. This is for the season that otherwise it would be very difficult for intermediaries like Google, Facebook etc, to act when millions of requests are made and the intermediary is then to judge as to which of such requests are legitimate and which are not. We have been informed that in other countries worldwide this view has gained acceptance, Argentina being at the forefront. Also, the court order and/or the notification by the appropriate Government or its agency must strictly conform to the subject matters laid down in Article 19(2). Unlawful acts beyond what Is laid down in Article 19(2) obviously cannot form any part of section 79. With these two caveats, we refrain from striking down section 79(3)(b).*

In ***Myspace Inc. v. Super Cassettes Industries Ltd***.[33] while deciding the issue of whether an entity is an intermediary or not; Division Bench held that Section 79 of the IT Act is not an - "enforceable provision", but merely provides – "affirmative defence" to entities which fulfil the criteria set forth therein. It was observed by the DB in the said case as under: —

*"51... The true intent of Section 79 is to ensure that in terms of globally accepted standards of intermediary liabilities and to further digital trade and economy, an intermediary is granted certain protections. Section 79 is neither an enforcement provision nor does it list out any penal consequences for noncompliance. It sets up a scheme where intermediaries have to follow certain minimum standards to avoid liability; it provides for an affirmative defence and not a blanket immunity from liability."*

[33] *Myspace Inc. v. Super Cassettes Industries Ltd,* FAO(OS) 540/2011, C.M. APPL.20174/2011, 13919 & 17996/2015, Delhi High Court, decided on 23 December, 2016.

### 5.4.2 PRESERVATION AND RETENTION OF INFORMATION BY INTERMEDIARIES

The Information Technology (Amendment) Act has made intermediaries responsible for preservation and retention of information. The term "information" includes data, message, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer-generated micro fiche [section 2(l)(v)] has been defined. The basic idea behind the introduction of this section is to preserve and retain electronic records for a sufficient period of time for certain post event requirements. In other words, every electronic record, which has been published or transmitted using any intermediary network will now be archived for a time period and in a format as prescribed by the Central Government.

It is obligatory to note that this section 67C[34] should be read with section 7 of the Act, as the latter lays down the following conditions for retention of electronic records:

(a) accessibility so as to be usable for a subsequent reference;

(b) retention in the format in which it was originally generated, sent or received or in a format, which can be demonstrated, to represent accurately the information originally generated, sent or received; and

(c) the details which will facilitate the identification of the origin, destination, date and time of despatch or receipt of such electronic record. This clause will not be applicable to any information, which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

### 5.4.3 PRESERVATION & RETENTION OF INFORMATION

In the past, there have been concerted efforts to implement section 67 of the Act. A major success came when a small step was taken in the form of issuance of an advisory on functioning matrimonial websites.[35] This advisory specifically mentioned:

*Matrimonial Website should store the IP address of profile creation and access*

[34] The Information Technology Act, 2000 (Act 21 of 2000) s. 67C read as - *Preservation and Retention of information by intermediaries. —*
(1) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.
(2) Any intermediary who intentionally or knowingly contravenes the provisions of sub-section (1) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

[35] Advisory on functioning of Matrimonial Website, etc. in accordance with the Technology Act and Rules made thereunder. Issued on 6 June 2016.

*logs (date and time stamping) for a period of one year from the date of account deactivation.*

The most significant step so far has been the notification of the Information Technology (Preservation & Retention of Information by Intermediaries Providing Digital Locker; Facilities) Rules, 2016[36] under section 67C of the Act.) Digital locker provides for a system which act as web and mobile based portal for providing preservation and retention of machine readable, printable, shareable, verifiable and secure state or central department or agency or body corporate issued electronic records. Any individual who is resident of India can able to open his digital locker account. Digital locker portal provides access to repositories and access gateway for issuers to issue and requesters to access digitally signed or equivalently authenticated electronic records.

### 5.4.4 INTERCEPTION & MONITORING OF ELECTRONIC COMMUNICATIONS

The law on interception in India derives its strength from the Indian Telegraph Act, 1885. Section 5(2)[37] of the said Act provides:

This section mirrors under what circumstances, the Central or a State Governments shall intercept any telegraph. Moreover, section 7(2) (b) provides for procedural safeguards *vis-à-vis* application of section 5(2) of the Act.

In fact, it was in ***R.M. Malkani v. State of Maharashtra[38]*****,** wherein it was held:
*...Article 21 contemplates procedure established by law with regard to deprivation of life or personal liberty. The telephonic conversation of an innocent citizen will be*

[36] Notified on 21 July 2016. These rules have been framed in exercise of the powers conferred by sub-section (1) of section 87 and clause (x) of sub-section (2) of section 87 read with section 6A and section 67C of the Information Technology Act, 2000.

[37] The Indian Telegraph Act, 1885 (Act 13 of 1885), s. 5(2) read as - On the occurrence of any public emergency or in the interest of the public safety, the Central or a State Government or any officer specially authorised in this behalf by the Central or a State Government, may, if satisfied that it is necessary or expedient so to do in the interests of sovereignty and integrity of India, the security of the State, friendly relations with Foreign States or public order or for preventing incitement to the commission of an offence for reasons to be recorded in writing, by order, direct that any message or class of messages to or from any person or class or persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order.

[38] *R.M. Malkani v. State of Maharashtra,* (1973) 1 SCC 471.

*protected by courts against wrongful or highhanded interference by tapping the conversation. The protection is not for the guilty citizen against the efforts of the police to vindicate the law and prevent corruption of public servants. It must not be understood that the courts will tolerate safeguards for the protection of the citizen to be imperilled by permitting the police to proceed by unlawful on irregular methods.*

No such procedural safeguards were framed, till 1997. The question posed above considered again in detail by the Hon'ble Supreme Court in ***Peoples Union for Civil Liberties (PUCL) v. UOI***[39]**,** wherein it was held as under:

*...so far as the power to intercept messages/conversations is concerned, the section clearly lays down the situations/conditions under which it can be exercised. But the substantive law as laid down in section 5(2) of the Act must have procedural backing so that the exercise of power is fair and reasonable. The said procedure itself must be just, fair and reasonable. "Procedure" must rule out anything arbitrary, freakish or bizarre. A valuable constitutional right can be canalised only by civilised processes.*

*No rules have been framed under section 7(2) (b) of the Act for providing the precautions to be taken for preventing the improper interception or disclosure of messages. In the absence or just and fair procedure for regulating the exercise of power under section 5(2) of the Act, it is not possible to safeguard the rights of the citizens guaranteed under Articles 19(1)(a) and 21 of the Constitution of India"... and till the time the Central Government lays down just, fair and reasonable procedure under section 7(2)(b) of the Act, it is necessary to lay down procedural, safeguards for the exercise of power under section 5(2) so that the right to privacy of a person is protected.*

Furthermore, the Supreme Court issued procedural directions to be followed by the competent authority for initiating telephone tapping:

Spurred by the Court's directions rule 419A was inserted[40] in the Indian Telegraph 1951. The said rule was in fact verbatim copy of the Courts directions. Subsequent Indian Telegraph (Amendment) Rules, 2007 amended the rule 419A from the point of view of further procedural clarity.[41]

The interception of conversation though constitutes an invasion of an individual right to privacy but the said right can be curtailed in accordance with procedure validly

[39] *Peoples Union for Civil Liberties (PUCL) v. UOI,* (1997) 1 SCC 301.
[40] Ins. By G. S. R. 123(E), dated 16th February, 1999.
[41] Ins. By G. S. R. 193(E) dated 1st March, 2007.

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. *Bhavesh* ***Jayanti Lakhani v. State of Maharashtra***[42]**,** the Hon'ble Supreme Court held that surveillance *per se* under the provisions of Delhi Special Police Establishment Act, 1946 may not violate individual or private rights including the right to privacy. However, it lamented that no such guidelines have been laid down in respect of surveillance conducted pursuant to a Red Corner or Yellow Corner Notice issued by Interpol.

As articulated above, interception of any message or class of messages are regulated under the telegraph Act, 1885. However, a piquant situation arose with the coming into effect of the Information Technology Act, 2000, as under this Act, the Controller of Certifying Authorities had been given the mandate to intercept any information transmitted through any computer resource under section 69.

Section 69 could have been seen as violative of Constitutional guarantees ("right to freedom of speech and expression" under article 19(1)(a) and "right to privacy" under article 21) as there were no safeguards established under the said section. In view of increasing complexities related to electronic communication and the accompanying

[42] *Bhavesh Jayanti Lakhani v. State of Maharashtra,* (2009) 9 SCC 551.

dangers, it was felt by the lawmakers to split the earlier section 69[43], into three separate sections, namely, sections 69, 69A[44] and 69B[45].

[43] The Information Technology Act, 2000 (Act 21 of 2000) s. 69 read as - *Powers to issue directions for interception or monitoring or decryption of any information through any computer resource.*— (1) Where the central Government or a State Government or any of its officer specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information transmitted received or stored through any computer resource.

(2) The Procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.

(3) The subscriber or intermediary or any person in charge of the computer resource shall, when called upon by any agency which has been directed under sub section (1), extend all facilities and technical assistance to-

(a) provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or intercept or monitor or decrypt the information, as the case may be; or

(c) provide information stored in computer resource.

(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine.

[44] The Information Technology Act, 2000 (Act 21 of 2000) s. 69A read as - *Power to issue directions for blocking for public access of any information through any computer resource* — (1) Where the Central Government or any of its officer specially authorised by it in this behalf is satisfied that it is necessary or expedient so to do, in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-section (2) for reasons to be recorded in writing, by order, direct any agency of the Government or intermediary to block for access by the public or cause to be blocked for access by public any information generated, transmitted, received, stored or hosted in any computer resource.

(2) The procedure and safeguards subject to which such blocking for access by the public may be carried out, shall be such as may be prescribed.

(3) The intermediary who fails to comply with the direction issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine.

[45] The Information Technology Act, 2000 (Act 21 of 2000) s. 69B read as - *Power to authorise to monitor and collect traffic data or information through any computer resource for Cyber Security.*— (1) The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorise any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.

(2) The Intermediary or any person in-charge of the computer resource shall when called upon by the agency which has been authorised under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.

(3) The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.

(4) Any intermediary who intentionally or knowingly contravenes the provisions of sub-section (2) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

*Explanation* – For the purposes of this section

(i) "Computer Contaminant" shall have the meaning assigned to it in section 43.

The constitutional validity of section 69A was challenged along with section 66A before the Supreme Court in ***PUCI v. UOI***[46] and ***Anoop M.K. v. UOI***[47]**.** Subsequently these petitions were tagged with the *Shreya Singhal* matter. Section 69A was also challenged before the Bombay High Court in ***Hindu Janjagruti Samiti v. UOI***[48] and before the Karnataka High Court in ***ISKCON, Bangalore v. UOI***[49]**.**

Over a period of time, blocking requests under section 69A have grown exponentially. Petitioners' increasingly invoking writ jurisdiction and even seeking removal of defamatory posts under section 69A. Surprisingly, the courts have so far been quite indulgent in this regard. In ***Rahul@Biswajit Sinha v. State of Bengal***[50]**,** the Calcutta High Court directed not only the removal of a news item as sought by the aggrieved petitioner but also ordered the blocking of the online news portal called Biswa Bangla Sambad. However, in ***Facebook Inc. v. The State of West Bengal***[51] the Kolkatta High Court stayed the order of the Chief Metropolitan Magistrate, Kolkatta issued under section 69A. Blocking directions under section 69A have been sought to (a) ban PUBG online game, and (b) ban the use of Zoom applications for official and personal purposes by the public[52]. The blocking of websites under section 69A has also been challenged[53].

A Public Interest Litigation - ***Sangeeta Gupta v. UOI***[54] was disposed of by the Allahabad High Court. Petitioner has contended before the court that "... the web series is offending to the principles of 'Sanatan Dharm' and is also in violation of fundamental rights enshrined under Articles 25 and 26 of the Constitution of India."

The Allahabad High Court observed:

*Having considered the nature of the relief claimed, we deem it appropriate to keep it open for the petitioner to agitate his cause before the competent authority of the Government of India. The writ petition hence is disposed of by giving liberty to the*

(ii) "traffic data" means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communication origin, destination, route, time, date, size, duration or type of underlying service or any other information.

[46] *PUCL v. UOI*, W.P. (C) No. 199 of 2013, decided on 24 March 2015.
[47] *Anoop M.K. v. UOI*, W.P. (Crl.) No. 196 of 2014.
[48] *Hindu Janjagruti Samiti v. UOI*, W.P. (C) No. 5255 of 2013.
[49] *ISKCON, Bangalore v. UOI*, W.P. (C) No. 5655 of 2013.
[50] *Rahul@Biswajit Sinha v. State of Bengal*, W.P. No. 4483(W) of 2018.
[51] *Facebook Inc. v. The State of West Bengal*, C.R.R. No. 2332 of 2017.
[52] *Harsh Chugh v. UOI*, WP© No. 10980 of 2020 presently pending before the Delhi High Court.
[53] *Tanul Thakur v. UOI*, Writ Petition No. 13037 of 2017 presently pending before the Delhi High Court.
[54] *Sangeeta Gupta v. UOI*, PIL No. 743 of 2020, decided on 28 September 2020.

*petitioner to approach the competent authority for redressal of his grievance.*

On June 29, 2020 the Government of India banned 59 apps of Chinese origin[55], invoking powers under Section 69A of the Information Technology Act read with relevant provisions of the Information Technology (Procedure and Safeguards for Blocking of Access of Information by Public) Rules, 2009. The rationale behind banning these apps was data security, security and national sovereignty concerns. These apps include as TikTok, SHAREIt, UC Browser, CamScanner, Helo, Weibo, WeChat and Club Factory etc.

Mr. Ravi Shanker Prasad, the Union Minister for Communication, Electronics and Information Technology and Law and Justice asserted that the 'digital strike' was done "for safety, security, defence, sovereignty & integrity of India and to protect data & privacy of citizens of India".[56]

## 5.5 PRIVACY & DATA PROTECTION LEGISLATION IN INDIA

India does not have any specific data preservation mechanism. Statutory protection of privacy can be found in India and is scattered across a number of statutes. The Information Technology Act 2000 (IT Act), as amended by the Information Technology (Amendment) Act 2008 (ITAA), has the broadest scope. The IT Act 2000 includes the most significant Indian statutory provisions dealing with data privacy issues, but only in a small number of sections, particularly sections 43 and 43A. It also deals with electronic transactions and digital signatures and cyber-security issues. The ITAA came into force on 27 October 2009.[57]

India did not have any general data protection legislation until December 2021, when a set of Rules (delegated legislation) made under section 43A of the IT Act purported to create a whole data privacy regime, but only by delegated legislation, not by primary legislation. These Rules superficially resemble a data protection law, but they have crippling deficiencies and ambiguities, they may be ultra vires; half of the Rules only apply to a very restrictive definition of' 'sensitive personal data', and not to other personal data; half of them do not impose obligations in relation to data subjects

[55] Press release issued by The Ministry of Electronics and information Technology, Government of India, *available at:* https://www.pib.gov.in/PressReleseDetailm.aspx?PRID=1635206 (last visited on May 30, 2022).
[56] "The impact of the Chinese apps ban" *The Hindu,* July 5, 2020.
[57] Notice under s. 1(2) ITAA (India), *The Gazette of India,* 27 October 2009.

per se, but only to 'the, provider of the information' and it is questionable whether and when consumers (data subjects) are given a right of civil action[58].

A few of the sections of IT act deal with privacy and data protection are as follows:

### 5.5.1 PRESERVATION AND RETENTION V. PRIVACY ISSUES

Since, any activity on the part of intermediaries to preserve and retain any information also require fulfilment of norms related to information (data) security and privacy, *i.e.,* the onus is on the intermediaries to have "reasonable security practices and procedures." Moreover, intermediaries are "body corporate" as defined under section 43A.

Also, section 43A has made it abundantly clear that where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

In other words, intermediaries shall have twin responsibilities, *i.e.,* to preserve and retain any information, as well as to implement and maintain reasonable security practices and procedures. Non-compliance of these provisions may attract criminal as well as civil liabilities under sections 67C and 43A respectively.

### 5.5.2 STING OPERATIONS UNDER SECTION 66E OF IT ACT

Sting operation by a private person or an agency, which may result in violating bodily privacy of another person will fall under section 66E[59] of the Act. Whatever may

---

[58] Graham Greenleaf, *Asian Data Privacy Laws Trade and Human Rights Perspective,* 413 (Oxford University Press, United Kingdom, 2017).

[59] The Information Technology Act, 2000 (Act 21 of 2000) s. 66E read as - *Punishment for violation of privacy* —Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both. *Explanation* — For the purposes of this section — (a) "transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons; (b) "capture", with respect to an image, means to videotape, photograph, film or record by any means;

(c) "private area" means the naked or undergarment clad genitals, public area, buttocks or female breast;

(d) "publishes" means reproduction in the printed or electronic form and making it available for public;

(e) "Under circumstances violating privacy" means circumstances in which a person can have a reasonable expectation that- (i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or (ii)any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place. The instances of violation of privacy may include installation of spycams/hidden cameras/communication device inside washrooms,

be the reason - public interest or the people right to know, one should not disregard the protection being given to an individual against his bodily privacy under this section.

In ***Court on its own motion v. State***[60] the Division Bench of the Hon ble Delhi High Court summarised its view on sting operations as follows:

1. A sting operation by a private person or agency is, by and large, unpalatable or unacceptable in a civilized society. A sting operation by a state actor is also unacceptable if the State actor commits an offence so that an offence by another person is detected.
2. A State actor or a law enforcement agency may resort to hidden camera or sting operations only to collect further or conclusive evidence as regards the criminality of a person who is already suspected of a crime.
3. The law enforcement agency must maintain the original version of the actual sting operation. Tampering with the original video or audio clips of a sting operation may lead to a presumption of the spuriousness of the entire operation.
4. A sting operation cannot be initiated to induce or tempt an otherwise innocent person to commit a crime or entrap him to commit a crime.
5. Normally, if a private person or agency unilaterally conducts a sting operation, it would be violating the privacy of another person and would make itself liable for action at law.
6. A sting operation must have the sanction of an appropriate authority. Since no such authority exists in India, and until it is set up, a sting operation by a private person or agency, ought to have the sanction of a court of competent jurisdiction which may be in a position to ensure that the legal limits are not transgressed, including trespass, the right to privacy of an individual or inducement to commit an offence etc.

Hence in view of aforesaid judgment, any sting operation, if it violates bodily privacy of another person, such a private person or agency conducting any such sting operation would be making itself liable for action at law.

bedrooms, changing rooms, hotel rooms, etc. for the purpose of violating bodily privacy of any user/occupant of such.

[60] *Court on its own motion v. State*, W.P. (CRL) No. 796/2007, decided on 21 August 2008.

### 5.5.3 PUBLISHING OR TRANSMITTING OBSCENE MATERIAL IN ELECTRONIC FORM

Section 67[61] of IT Act prescribes punishment for publishing or transmitting obscene material in electronic form.

In terms of everyday application, this section covers websites, graphic files, such as .GIF and .JPEG images (downloaded from FTO sites, embedded in web pages), text messages (Email, SMS, Chat-rooms, BBS), audio/sound messages (Net-telephony, music downloads), digital photographs (MMS, PNG or JPG digital format[62]), pseudo-photographs[63] (morphed images), deepfake[64], software programs, video calls etc.

In ***Avnish Bajaj v. State*** [65] (Bazee Case) the court opined that the entire text of the listing (as given under point no. 3) – "prima facie it appears that the listing itself answered the definition of obscenity since it contained words or writing that appealed "to the prurient interest" or if taken as a whole was "such as to tend to deprave or corrupt person, who is likely to read, see or hear the matter contained or embodied in it." The listing contained explicit words that left a person in no doubt that what was sought to be sold was lascivious. The words "This video is of a girl of DPS RK PURAM which has been filmed by his boyfriend in very sexually explicit conditions" are a prominent feature of the listing which invited a potential buyer to purchase the obscene object which was the video clip by projecting it as child pornography since the reference is to school children."

In appeal before the findings of the Delhi High Court that though charge has not been made out under section 67 of the IT Act, yet the accused could be proceeded under section 292 IPC, the Supreme Court in **Sharut Babu Digumarti v. Govt. of NCT of**

---

[61] The Information Technology Act, 2000 (Act 21 of 2000) s. 67 read as - *Punishment for publishing or transmitting obscene material in electronic form* — Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees.

[62] Camera phones take pictures either in PNG or JPG format.

[63] Pseudo-photograph means an image, whether made by computer-graphics or otherwise however, which appears to be a photograph. Thus, a pseudo-photograph means any image that is capable of being resolved into an image that appears to be a photograph and, if the image appears to be shown a child, then the image is to be treated as if that of a child.

[64] Existing image or video is replaced with someone else's likeness.

[65]

**Delhi**[66] held:

It has to be borne in mind that IT Act is a special enactment. It has special provisions. Section 292 of the Indian Penal Code makes offence sale of obscene books, etc. but once the offence has a nexus or connection with the electronic record the protection and effect of section 79 cannot be ignored or negated. We are inclined to think so as it is a special provision for a specific purpose and the Act has to be given effect to as to make the protection effective and true to legislative intent.

… We have also referred to sections 79 and 81 of the IT Act. Once the special provisions having the overriding effect do cover a criminal act and the offender, he gets out of the net of the Indian Penal Code and in this case, section 292. It is apt to note here that electronic forms of transmission are covered by the IT Act, which is a special law. IT is settled position in law that a special law shall prevail over the general and prior laws. When the Act in various provisions deals with obscenity in electronic form, it covers the offence under section 292 Indian Penal Code.

…. We are of the considered opinion that the High Court has fallen into error that though charge has not been made out under section 67 of the IT Act, yet the Appellant could be processed under section 292 Indian Penal Code.

Publication or transmissions in the electronic form includes dissemination, storage and transmission of information or data in electronic form. In view of the ease with which obscene content can be replicated, misused, and distributed over the Internet using all kinds of information technology and communications tools – it was felt by the lawmakers to move beyond "likely audience" test of section 67 and to provide more stringent mechanism to combat obscenity in electronic form. To serve this purpose section 67A[67] was inserted in IT Act.

Supreme Court in ***Kamlesh Vaswani v. UOI***[68]**,** has been approached to direct the respondents to block the pornography websites, platforms, links or downloading by whatever other internet means or name in order to prevent easy access whether in

[66] *Sharut Babu Digumarti v. Govt. of NCT of Delhi*, (2017) 2 SCC 18: AIR 2017 SC 150.
[67] The Information Technology Act, 2000 (Act 21 of 2000) s. 67A read as *Punishment for publishing or transmitting of material contains sexually explicit act, etc, in electronic form.*—Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to live years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.
[68] *Kamlesh Vaswani v. UOI*, (2016) 7 SCC 592.

private or public. During the proceedings before the court, the respondent did block 857 websites, allegedly depicting child pornography content but had to hastily withdraw the order as majority of the listed websites on examination found to carry only adult pornography content. Nevertheless, this case led to certain long term of regulating child pornography in India, namely blocking of child pornography content based on Internet Watch Foundation (IWF) list, POCSO E-box for receiving online complaints, etc.

In this context, it would be imperative to discuss ***Prajwala case***[69]**,** which led to a serious attempt on the part of the Supreme Court bench headed by Justice Madam B. Lokur and Justice Uday Umesh Lalit to bring on board various Central Ministries' (Ministry of Home, Ministry of Electronics & Information Technology, and Ministry of Women and Child Development). State Governments, Intermediaries (Google, Microsoft, Facebook, WhatsApp), and Technical experts from India and abroad to tackle the menace of obscene images/rape videos/child sexual images on the internet.

### 5.5.4 PROTECTING PRIVACY DURING COVID-19 PANDEMIC

Protecting individuals[70] privacy during COVID-19 pandemic proved to be a herculean task as the medical emergency of humungous proportion has taken a toll of hundreds and thousands of lives. The health response which was implemented across the states, districts, metropolitan areas, and hinterland was based on collection of sets of data, referred to as 'response data; which includes[71]:

(a) demographic data (means the name, mobile number, age, gender, profession, and travel history of an individual),

(b) contact data (means data about any other individual that a given individual has come in close proximity with, including the duration of the contact, the proximate distance between the individuals and the geographical location at which the contact occurred),

(c ) self-assessment data (means the responses provided by that individual to the self-assessment test administered within the Arogya Setu mobile application),

[69] Prajwala Letter dated 18.2.2015 Video of Sexual Violence and Recommendations, Re, Suo Moto Writ Petition (Crl.) 3 of 2015. Presently Pending before the Supreme Court.
[70] Individual herein means persons who are infected, at high risk of being infected or who have come in contact with infected individuals.
[71] *Supra* note 21 at 305.

(d) location data (means data about the geographical position of an individual in latitude and longitude).

Arogya Setu App for mobile and hand-held devices was operationalised to assist the state authorities to collect and access the response data of individuals as identified above. On 11 May, 2020 the Ministry of Electronics & Information Technology notified the Protocol[72]. The developer of Aarogya Setu, i.e., the National Informatics Centre is made responsible for collection, processing and managing 'response data' collected by the Aarogya Setu mobile application.

In the early days of COVID-19, the courts came to the rescue of the common man by upholding the rights of individuals vis-à-vis State authorities. In ***Balu Gopalakrishnan v. State of Kerla***[73] (also known as ***Sprinklr case)***, the High Court of Kerala (Ernakulum Bench) in its thought-provoking order set up the templates for COVID-19 to ensure that there is no "data epidemic" after the COVID-19 epidemic is controlled.

The researcher feels is pertinent to mention here that section 72[74] and 72A[75] of the Information Technology Act, 2000 talk about the penalty for breach of confidentiality and privacy & punishment for disclosure of information in breach of lawful contract respectively. To bring the intermediary in the ambit of punishment in case violates users' privacy, section 72A[76] was inserted in Information Technology Act, 2000.

---

[72] https://www.meity.gov.in/writereaddata/files/Aarogya_Setu_data_access_knowledge_Protocol.pdf (last visited on May 30, 2022).

[73] W.P. (C), Temp. No. 84 of 2020, decided on 24 April 2020.

[74] The Information Technology Act, 2000 (Act 21 of 2000), s. 72 read as - *Penalty for Breach of confidentiality and privacy.*–Save as otherwise provided in this Act or any other law for the time being in force, if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

[75] The Information Technology Act, 2000 (Act 21 of 2000), s. 72A read as - *Punishment for disclosure of information in breach of lawful contract.*–Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both.]

[76] Inserted by Act of 10 of 2009, sec. 37 (w.e.f. 27.10.2009).

The issue of confidentiality and privacy as enumerated in sections 72 and 72A of the Act should be read along with the eight reasonable restrictions imposed by Article 19(2) on right "to freedom of speech and expression" an enumerated in Article 19(1)(a) of the Constitution of India. If need be, 'data subject' may take advantage of Article 21 which states that "no personal shall be deprived of his life and personal liberty except according to the procedure established by law".[77]

## 5.6 OTHER LEGISLATION RELEVANT TO DATA PROTECTION IN INDIA

There are other variety of Acts of some significance and effectiveness in data protection areas.

### 5.6.1 CREDIT INFORMATION COMPANIES (REGULATION) ACT 2005 — AN IGNORED LAW

In contrast, the Credit Information Companies (Regulation) Act 2005 (CICRA), operational since 2006[78], is the only Indian legislation, other than the IT Act, to provide a comprehensive data protection code. Despite the complexity of the Act, Regulations, and those Rules already published, none of them have any specific provisions for consumers to make complaints, receive assistance, or have remedies awarded in their favour.

### 5.6.2 THE PROTECTION OF HUMAN RIGHTS ACT, 1993

The Protection of Human Rights Act 1993 (PHRA) defines 'human rights' by reference to India's obligations under its Constitution and international commitments, and is therefore broad enough to include ICCPR Article 17 concerning privacy[79]. It establishes the National Human Rights Commission (NHRC)[80] which has the power to investigate alleged violations[81] and can recommend that the government or authorities pay compensation, commence prosecutions, and approach courts for directions, orders, or writs. It has no independent powers to take remedial actions. Complaints can also be

[77] *Supra* note 21 at 311.
[78] The Act was notified in the Gazette on 23 June 2005, and came into force by Notification on 14 December 2006. The rules and regulations were notified on the same day, making the Act operational.
[79] Protection of Human Rights Act (India), s. 1(d).
[80] Protection of Human Rights Act (India), s. 3.
[81] Protection of Human Rights Act (India), s. 12(a).

made to state Human Rights Commissions. The NHRC has not had any major involvement in data privacy issues, other than making submissions on the ID number, but it has had very significant involvement in Supreme Court decisions concerning compulsory DNA testing, lie detector tests, and related matters, with its guidelines having been adopted by the Supreme Court.[82] No privacy issues are included in the hundreds of cases heard by it and summarized on its website since 1993.[83] Its focus has been, and is, on wrongful deaths and other extreme violations.

However, there are other statutes which provide some safeguards to the lack of explicit legislation. The Recovery of Debts Due to Banks and Financial Institutions Act, 1993 (No. 51 of 1993), codifies India's tradition of maintaining confidentiality in bank transactions. Privacy in telecommunications is regulated by the Telecom Regulatory Authority of India (TRAI). The Common Charter of Telecom Services for adoption by all Telecom Service providers stipulates that "all Service Providers assure that the privacy of their subscribers (not affecting the national security) shall be scrupulously guarded". Certain older laws are also relevant. The Indian Contract Act, 1872 (No. 9 of 1872), offers an alternative solution to protect data as Indian companies acting as "data importers" may enter into contracts with "data exporters" to adhere to a high standard of data protection. The Specific Relief Act, 1963 (No. 47 of 1963), provides preventive relief in the form of temporary and perpetual injunctions in order to prevent the breach of an existent obligation, whether expressly or by implication. However, the outcomes, though, depend on judicial interpretation. The Indian Telegraph Act, 1885, No. 13 of 1885, recognises privacy as a right but the Government has the power to intercept communication for national security.

## 5.7 PRIVACY JUDGEMENT (PUTTASWAMY V UOI[84]) AS A GUIDING TOOL

This landmark judgment fundamentally changed the way in which the government viewed its citizens' privacy, both in practice and prescription.

1. It requires governments to undertake structural reforms and bring transparency and openness in the process of commissioning and executing its surveillance projects, and build a mechanism of judicial oversight over surveillance requests.

[82] *Selvi v. State of Karnataka*, (2010) 7 SCC 263.
[83] NHRC website www.nhrc.nic.in, See 'Human Rights cases' and 'Suo-Motu Cases'.
[84] *Supra* note 1.

2. It demands from the authorities to demonstrate great care and sensitivity in dealing with the personal information of its citizens.
3. It requires to legislate a transformative, rights-oriented data protection law that holds all-powerful entities that deal with citizens' personal data (data controllers), including the state, accountable.

Various steps have been taken by the Government of India to strengthen privacy regime. Some of them are as follows:

### 5.7.1 JUSTICE B N SRIKRISHNA COMMITTEE

The government of India appointed a committee of experts for Data protection under the chairmanship of Justice B N Srikrishna that submitted its report[85] in July 2018 along with a draft Data Protection Bill[86]. The Report has a wide range of recommendations to strengthen privacy law in India. Its proposals included restrictions on processing and collection of data, Data Protection Authority, right to be forgotten, data localisation, explicit consent requirements for sensitive personal data, etc.

The Justice Srikrishna Committee in its White Paper has also suggested a few ways in which jurisdiction can be ascertained. of the three alternatives suggested, the first one refers to data stored on servers located within the territorial limits of India- which has been dealt with later on in the paper. Under the second method, the scope of extraterritorial laws is decided on the basis of an enquiry of the entity carrying out a business in India in a consistent manner with the aim of profit. In the third method, the conduct of the service provider in offer is used as the determinative factor. Both the classifications are based on determining the intention of the parties involved.

### 5.7.2 PERSONAL DATA PROTECTION BILL, 2019

The Personal Data Protection Bill, 2019 was introduced in Lok Sabha by the Minister of Electronics and Information Technology, Mr. Ravi Shankar Prasad, on December 11, 2019. The Bill seeks to provide for protection of personal data of individuals, and establishes a Data Protection Authority for the same.[87]

[85] B. N. Srikrishna *available at:* https://en.wikipedia.org/wiki/B._N._Srikrishna (last visited on May 30, 2022).
[86] https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf
87 The Personal Data Protection Bill, 2019 https://prsindia.org/billtrack/the-personal-data-protection-bill-2019 (last visited on May 30, 2022).

### 5.7.3 SALIENT FEATURES OF PERSONAL DATA PROTECTION BILL, 2019

The bill aims to protect the privacy of individuals relating to their personal data, develop trust between persons and entities processing the personal data, protect the rights of individuals whose personal data are processed, laying down norms for social media intermediary, cross-border flow of data, remedies for unauthorised and harmful processing, for the said purpose and for matters connected therewith establishment of data protection authority is must. The bill emphasized as the right to privacy is a fundamental right so it is necessary to protect personal data as an essential facet of information privacy.

Section 3 'definition clause' in chapter I covers biometric data[88], data[89], data fiduciary[90], data principal[91], personal data[92], processing[93], profiling[94], sensitive data[95], etc.

Chapter II of aforesaid bill talks about 'Obligation of Data Fiduciary' which includes different data protection principles adopted by the world community in their legislation. Section 4 prohibits processing of data except for any specific, clear and

[88] The Personal Data Protection Bill, 2019, s. 3 (7) read as *"biometric data"* means facial images, fingerprints, iris scans, or any other similar personal data resulting from measurements or technical processing carried out on physical, physiological, or behavioural characteristics of a data principal, which allow or confirm the unique identification of that natural person.

[89] The Personal Data Protection Bill, 2019, s. 3 (11) read 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.

[90] The Personal Data Protection Bill, 2019, s. (13) read as *"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.

[91] The Personal Data Protection Bill, 2019, s. 3 (14) read as *"data principal"* means the natural person to whom the personal data relates.

[92] The Personal Data Protection Bill, 2019, s. 3 (28) read 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.

[93] The Personal Data Protection Bill, 2019, s. 3 (31) read as *"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;

[94] The Personal Data Protection Bill, 2019, s. (32) read as *"profiling"* means any form of processing of personal data that analyses or predicts aspects concerning the behaviour, attributes or interests of a data principal.

[95] The Personal Data Protection Bill, 2019, s. 3 (36) read as *"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.

lawful purpose. Data processing shall be carried out in fair and reasonable manner in order to ensure the privacy of the data principal. The proposed principles in the bill are notice[96] in clear and concise language to all individuals by the data controller before personal information is collected. Section 8 talks about 'quality of personal data processed[97].' Certain restrictions have been imposed on data fiduciary under section 9[98] of the bill. Under section 10 of the bill data fiduciary's accountability has been fixed while processing data. As per section 11 of the bill it is mandatory to seek the consent of data principal before processing of personal data and the consent received must be as per the law.

[96] The Personal Data Protection Bill, 2019, s. 7. (1) read as - Every data fiduciary shall give to the data principal a notice, at the time of collection of the personal data, or if the data is not collected from the data principal, as soon as reasonably practicable, containing the following information, namely:— (a) the purposes for which the personal data is to be processed; (b) the nature and categories of personal data being collected; (c) the identity and contact details of the data fiduciary and the contact details of the data protection officer, if applicable; (d) the right of the data principal to withdraw his consent, and the procedure for such withdrawal, if the personal data is intended to be processed on the basis of consent; (e) the basis for such processing, and the consequences of the failure to provide such personal data, if the processing of the personal data is based on the grounds specified in sections 12 to 14; ( f ) the source of such collection, if the personal data is not collected from the data principal; (g) the individuals or entities including other data fiduciaries or data processors, with whom such personal data may be shared, if applicable; (h) information regarding any cross-border transfer of the personal data that the data fiduciary intends to carry out, if applicable; (i) the period for which the personal data shall be retained in terms of section 9 or where such period is not known, the criteria for determining such period; ( j) the existence of and procedure for the exercise of rights mentioned in Chapter V and any related contact details for the same; (k) the procedure for grievance redressal under section 32; (l) the existence of a right to file complaints to the Authority; (m) where applicable, any rating in the form of a data trust score that may be assigned to the data fiduciary under sub-section (5) of section 29; and (n) any other information as may be specified by the regulations. (2) The notice referred to in sub-section (1) shall be clear, concise and easily comprehensible to a reasonable person and in multiple languages where necessary and practicable. (3) The provisions of sub-section (1) shall not apply where such notice substantially prejudices the purpose of processing of personal data under section 12.

[97] The Personal Data Protection Bill, 2019, s. 8. (1) read as - The data fiduciary shall take necessary steps to ensure that the personal data processed is complete, accurate, not misleading and updated, having regard to the purpose for which it is processed. (2) While taking any steps under sub-section (1), the data fiduciary shall have regard to whether the personal data— (a) is likely to be used to make a decision about the data principal; (b) is likely to be disclosed to other individuals or entities including other data fiduciaries or processors; or (c) is kept in a form that distinguishes personal data based on facts from personal data based on opinions or personal assessments. (3) Where personal data is disclosed to any other individual or entity, including other data fiduciary or processor, and the data fiduciary finds that such data does not comply with the requirement of sub-section (1), the data fiduciary shall take reasonable steps to notify such individual or entity of this fact.

[98] The Personal Data Protection Bill, 2019, s. 9. (1) read as - The data fiduciary shall not retain any personal data beyond the period necessary to satisfy the purpose for which it is processed and shall delete the personal data at the end of the processing. (2) Notwithstanding anything contained in sub-section (1), the personal data may be retained for a longer period if explicitly consented to by the data principal, or necessary to comply with any obligation under any law for the time being in force. (3) The data fiduciary shall undertake periodic review to determine whether it is necessary to retain the personal data in its possession. (4) Where it is not necessary for personal data to be retained by the data fiduciary under sub-section (1) or sub-section (2), then, such personal data shall be deleted in such manner as may be specified by regulations.

Chapter II talks about grounds for processing of personal data when consent is not required. Section 12, 13 and 14 provide other legal bases for processing of personal data. These include, under section 12, public functions authorised by law, and to respond to medical emergency or threat to public health. Section 13 provides for processing necessary in an employment context. Section 14 permits processing without consent, if necessary, for 'reasonable purposes' as may be specified by the Regulations, taking into account respective private and public interests, whether it is reasonable to expect consent to be obtained, and the reasonable expectations of the data principal in the context.

Chapter IV talks about personal data and sensitive personal data of children. Chapter V highlights rights of data principal. These rights include right to confirmation and access[99]; right to correction and erasure[100]; right to data portability[101], right to be forgotten[102], etc. Chapter VI deals with transparency and accountability measures to be taken by data fiduciary. According to section 22 every data fiduciary shall adopt a privacy by design policy[103], submit it privacy by design policy to the data authority for

[99] The Personal Data Protection Bill, 2019, s. 17. (1) read as - The data principal shall have the right to obtain from the data fiduciary— (a) confirmation whether the data fiduciary is processing or has processed personal data of the data principal; (b) the personal data of the data principal being processed or that has been processed by the data fiduciary, or any summary thereof; (c) a brief summary of processing activities undertaken by the data fiduciary with respect to the personal data of the data principal, including any information provided in the notice under section 7in relation to such processing. (2) The data fiduciary shall provide the information under sub-section (1) to the data principal in a clear and concise manner that is easily comprehensible to a reasonable person. (3) The data principal shall have the right to access in one place the identities of the data fiduciaries with whom his personal data has been shared by any data fiduciary together with the categories of personal data shared with them, in such manner as may be specified by regulations.

[100] The Personal Data Protection Bill, 2019, s. 18. (1) read as - 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.

[101] The Personal Data Protection Bill, 2019, s. 19. (1) Where the processing has been carried out through automated means, the data principal shall have the right to— (a) receive the following personal data in a structured, commonly used and machine-readable format— (i) the personal data provided to the data fiduciary; (ii) the data which has been generated in the course of provision of services or use of goods by the data fiduciary; or (iii) the data which forms part of any profile on the data principal, or which the data fiduciary has otherwise obtained; and (b) have the personal data referred to in clause (a) transferred to any other data fiduciary in the format referred to in that clause.

[102] The Personal Data Protection Bill, 2019, s. 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.

[103] The Personal Data Protection Bill, 2019, s. 22 of the bill states that (c) the technology used in the processing of personal data is in accordance with commercially accepted or certified standards; (d) the

certification, ensures transparency in processing of personal data (section 23), takes security safeguards (section 24), reporting of personal data breach to the data authority by the data fiduciary. A data protection impact assessment by data fiduciary is necessary prior processing which may involve new technologies or large-scale profiling or use of sensitive personal data which carries a risk of significant harm to data principals (section 27). Section 30 deals with appointment of a data protection officer by significant data fiduciary with prescribed qualification and experience.

Chapter VII prohibits transfer of personal data outside India. As per section 33, the personal data may be transferred outside India, but such personal data shall be continued to be stored in India. For processing of sensitive personal data outside India, explicit consent of data principal for such transfer is required.

Chapter VIII empowers central government to exempt any agency of government from application of act. Chapter IX deals with establishment of data protection of authority, composition and qualification for appointment of members, terms and conditions of appointment, powers of chairperson, powers and functions of authority, code of practice, etc. Chapter X talks about penalties and compensation imposed on data fiduciary in case contravenes the provisions of the act. A provision of establishment of appellate tribunal by the central government by notification to redress the grievances of aggrieved parties has been covered under chapter XI of the bill.

The Parliamentary Committee presently considering the Bill is unbalanced in its composition with no diverse perspective present. Absence of dissent in the Committee with majority of the members aligned with the government view, steers the way free for the Bill to be passed with least or no amendments.

## 5.8 THE INFORMATION TECHNOLOGY (INTERMEDIARY GUIDELINES AND DIGITAL MEDIA ETHICS CODE) RULES, 2021

After years of discussions and debates, the Ministry of Electronics and Information Technology, Government of India in exercise of the powers conferred by section 79 (2) (c), section 69A (2) read with section 87 (1), section 87 (2) (z), (zg) of the Information Technology Act, 2000 (21 of 2000) has notified new rules for monitoring social media digital media platforms. The new rules, viz. Information

legitimate interests of businesses including any innovation is achieved without compromising privacy interests; (e) the protection of privacy throughout processing from the point of collection to deletion of personal data;

Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("**Intermediary Guidelines**")[104] *inter alia* aims to serve a dual-purpose: (1) increasing the accountability of the social media platforms (such as Facebook, Instagram, Twitter etc.) to prevent their misuse and abuse; and (2) empowering the users of social media by establishing a three-tier redressal mechanism for efficient grievance resolution.

### 5.8.1 NEED FOR REGULATING THE SOCIAL MEDIA PLATFORMS

India is claimed to be the world's "largest open Internet society" and attracts many social media companies to do business in India. However, there are a growing number of instances where social media is being used as a tool for violating the privacy of individuals through the accumulation of personal data of users in overt and covert means, mass circulation of obscene content, inciting malicious or anti-national 'fake news', inciting communal riots through disrespect to religious sentiments, interfere in election results. This abuse of social media is due to lack of due diligence observed by the intermediaries, robust complaint, and redressal mechanism which is inaccessible to the ordinary social/digital media users. It was therefore considered to set in motion a mechanism for consumer complaints and redressal powers, observance of due diligence in the form of Intermediary Guidelines. The Intermediary Guidelines are intended to be integrated into the existing information technology laws and regulate the social media and digital media platforms within India.[105]

The rationale behind the Intermediary Guidelines stems from a plethora of different orders and reports including the Calling Attention Motion on 'Misuse of Social Media platforms and spreading of fake news' admitted in the Rajya Sabha on July 26, 2018, the Hon'ble Supreme Court's order dated December 11, 2018 which observed that the Government of India should frame necessary guidelines to eliminate child pornography, rape etc. for content hosting platforms and other applications; the Hon'ble Supreme Court order dated September 24, 2019 directing the Ministry of Electronics and Information Technology to apprise the timeline in respect of completing the process of notifying the new rules, and lastly, the report of the Ad-hoc

[104]https://www.meity.gov.in/writereaddata/files/Intermediary_Guidelines_and_Digital_Media_Ethics_Code_Rules-2021.pdf (last visited on 30 May, 2022).
[105] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (prsindia.org)

committee of the Rajya Sabha[106] dated February 3, 2020 relating to the alarming issue of pornography on social media and its effect on children and society as a whole.

### 5.8.2 KEY FEATURES OF THE INTERMEDIARY GUIDELINES

The rules cover definitions of act[107], intermediary[108], significant social media intermediary[109], social media intermediary[110], etc. under definition clause.

Rule 4 puts obligations on intermediary including a social media intermediary to observe the prescribed due diligence measures in the course of discharging its duties. These due diligence measures *inter alia* include:

(a) The intermediary shall prominently publish on its website, mobile based application or both, the rules and regulations, privacy policy and user agreement for access or usage of its computer resource by any person.

(b) The intermediary through the rules and regulations, privacy policy/the user agreement should inform the user of its computer resource not to host, display, upload, modify, publish, transmit, store, update or share any information that *inter alia*:

(i) belongs to another person and to which the user does not have a right;

(ii) information is defamatory, obscene, pornographic, pedophilic, invasive of another's privacy, including bodily privacy, insulting or harassing on the basis of gender, libelous, racially or ethnically objectionable, relating or encouraging money laundering or gambling or otherwise inconsistent with or contrary to the laws in force;

(iii) is harmful to the minors;

(iv) infringes any patent, trademark, copyright or other proprietary rights;

---

106 https://rajyasabha.nic.in/rsnew/Committee_site/Committee_File/Press_ReleaseFile/71/140/295P_2020_2_15.pdf

107 Rule 2 (1) (c) 'Act' means the Information Technology Act, 2000 (21 of 2000).

108 Rule 2 (1) (m) 'Intermediary' shall have the same meaning as assigned to it in clause (w) of sub-section (1) of section 2 of the Act; *Explanation:* For the purpose of these rules, an intermediary includes websites, apps and portals of social media networks, media sharing websites, blogs, online discussion forums and other such functionally similar intermediaries.

109 Rule 2 (1) (y) 'significant social media intermediary' means a social media with users above such threshold as may be notified by the Central Government.

110 Rule 2 (1) (z) 'social media intermediary' means an intermediary referred to in clause (m) which primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services but shall not include an intermediary which primarily, — i. enables commercial or business-oriented transactions; or ii. provides access to internet or computer networks; or iii. is in the nature of a search-engine, on-line encyclopaedia, online directory or suggestion tool, e-mail service or online storage service.

(v) violates any law for the time being in force;

(vi) deceives or misleads the addressee about the origin of the message or knowingly and intentionally communicates any information which is patently false or misleading in nature but may reasonably be perceived as a fact; and

(vii) impersonates another person;

(viii) threatens the unity, integrity, defense, security or sovereignty of India, friendly relations with foreign States, or public order, or causes incitement to the commission of any cognizable offence or prevents investigation of any offence or in insulting another nation.

(c ) An intermediary shall periodically inform its users, at least once every year, that in case of non-compliance with rules and regulations, privacy policy or user agreement for access or usage of the computer resource of such intermediary, it has the right to terminate the access or usage rights of the users to the computer resource immediately or remove non-compliant information or both, as the case may be.

(d ) an intermediary, upon receiving a court order or upon being notified by the appropriate government or agency under the IT Act, shall not host, store or publish any unlawful information which is prohibited under any law for the time being in force in relation to the interest of the sovereignty and integrity of India, security of the state, friendly relations with foreign states, public order, decency or morality, in relation to contempt of court, defamation, incitement to an offence relating to the above or any information which is prohibited under any law for the time being in force.

(f ) The intermediary shall inform its users of its rules and regulations, privacy policy or user agreement periodically, at least once in a year, or whenever there is a change in the rules and regulations, privacy policy or user agreement, as the case may be.

(h) where an intermediary collects information from a user for registration on the computer resource, it shall retain the information for a period of 180 days after any cancellation or withdrawal of the registration, as the case may be.

(j ) the intermediary shall, immediately but not later than 72 hours of the receipt of an order, provide information under its control or possession, or assistance to the Government agency which is lawfully authorized for investigative or protective

or cyber security activities, for the purposes of verification of identity, or for the prevention, detection, investigation or prosecution, of offences under any law for the time being in force, or for cyber security incidents.

Apart from due diligence mentioned under rule 4, a social media intermediary is required to comply with certain additional due diligence measure as mentioned under rule 5, which *inter alia* include:

(a) appointing a chief compliance officer who will be responsible for ensuring compliance with the provisions of the IT Act and rules framed thereunder.

(b) appointment of a nodal contact person for 24x7 coordination with law enforcement agencies and officers to ensure compliance with their orders or requisitions.

(c) Appoint a Resident Grievance Officer, who shall be responsible for the functions referred to in clause (n) of sub-rule (1) of rule 4.

(d) publishing a compliance report every month mentioning the details of complaints received and action taken thereon, and the number of specific communication links or parts of information that the intermediary has removed or disabled access to in pursuance of any proactive monitoring conducted by using automated tools or any other relevant information, as may be specified.

A significant social media intermediary will endeavour to deploy technology-based measures, including automated tools or other mechanisms to proactively identify information that depicts any act or simulation in any form depicting rape, child sexual abuse or conduct, whether explicit or implicit, or any information which has been disabled on the computer resource of such intermediary.

A significant social media intermediary is required to have a physical contact address in India published on its website, mobile based application or both, for the purposes of receiving the communications addressed to it.

A social media intermediary is required to enable the user who register for the services from India, or use the services in India, to voluntarily verify their accounts by using any appropriate mechanism, including the active Indian mobile number of such users and where any user voluntarily verifies the account, such user shall be provided with a demonstrable and visible mark of verification, which shall be visible to all users of the service.

In the event of non-observance of the rules of Intermediary Guidelines by an intermediary, the provisions of sub-section (1) of section 79 of the IT Act will not be applicable to such intermediary and the intermediary will be liable for punishment under any law for the time being in force including in accordance with the provisions of the IT Act and the Indian Penal Code.

## 5.9 SOCIAL MEDIA AND THE INDIAN JUDICIARY

Social media has transformed the way society communicates. Its vast technological outreach is a great educational forum to garner knowledge, update skills, and open the mind and heart to the wonders of the world. There is no denying that the reach of social media presents unprecedented opportunities for judges and lawyers to stay connected with the community they serve. But there are risks and challenges inherent in the use of social media by the judiciary which highlights issues of integrity and ethics. Judges have to be extra vigilant and exercise selective restraint to perform the solemn duty in the 'Temple of Justice'.[111]

Union Law Minister Ravi Shankar Prasad while speaking in the "International Judges Conference" organized by the Supreme Court opined that

*"I am a great supporter of social media and freedom. I know it is empowering. but (there) is a dangerous trend. Judges must be left completely independent to give judgment as what they think is the correct mode in accordance with the rule of law."*[112]

***Matrimony.com Ltd. v. Google LLC (2018):*** After three years of rigorous investigation, the Competition Commission of India (CCI) has announced its landmark decision[113] against Google, holding Google guilty of contravention of competition law on three counts out of the many investigated and imposed a penalty of Rs. 135.86 crores upon Google. Information's against Google were filed by bharatmatrimony.com and Consumer Unity and Trust Society (CUTS) in 2012. CCI, by majority of 4:2, has held Google guilty of abusing its dominant position by indulging into search bias and for imposing certain restrictions upon its direct search intermediation partners.

***WhatsApp Privacy Policies -*** The latest update to the privacy policy proposed to be rolled out by WhatsApp (a Facebook group company) in January 2021 caused much

[111] https://www.barandbench.com/columns/social-media-and-the-judiciary.
[112] https://www.barandbench.com/columns/social-media-and-the-judiciary.
[113] *Matrimony.com Ltd. v. Google LLC,* 2018 SCC OnLine CCI 1.

backlash owing to what is perceived as platform users being arm-twisted into accepting into their terms of service and privacy policy. What made it different this time was that unlike previous updates to the privacy policy where users had the option to opt out, this time, WhatsApp has given the ultimatum of either accepting the revised terms, or exiting the messaging platform.[114]

Notwithstanding the absence of a real choice in the matter, the larger issue here is also the fact that the updated terms allow sharing of WhatsApp user data with the other Facebook companies. This data, as per the privacy policy, may include "account registration information (such as your phone number), transaction data, service-related information, information on how you interact with others (including businesses) when using our services, mobile device information, your IP address, and may include other information identified in the privacy policy section entitled "Information We Collect" or obtained upon notice to you or based on your consent".[115]

The broadly worded clause is cause for concern. Secondly, the policy is also said to be discriminatory considering that users in the European Union are not mandatorily subjected to these privacy terms. The situation is aggravated in light of the fact that India is WhatsApp's largest market.[116]

***Karmanya Singh Sareen v. Union of India (2016)*** - In 2016, WhatsApp changed its privacy settings and allowed Facebook to share data of the users. This policy was challenged in Karmanya Singh Sareen v. Union of India[117] in Delhi High Court. A special leave petition was filed but the Court directed that the Court can only decide when there is misuse of data and not on the possibility that the data will be misused. The Court directed that the users who do not wish to share their data can delete their accounts. The case was then brought in front of the Supreme Court where it is pending.

---

[114] FE Online, Trouble Mounts for WhatsApp as India Starts "Evaluating" Controversial New Privacy Policy Update,
Financial Express *available at:* https://www.financialexpress.com/industry/technology/trouble-mounts-for-whatsapp-as-india-starts-evaluating-controversial-new-privacy-policy-update/2171023, (last visited on May 30, 2022).

[115] WhatsApp, What Information does WhatsApp Share with the Facebook Companies?, WhatsApp *available at:*
https://faq.whatsapp.com/general/security-and-privacy/what-information-does-whatsapp-share-with-thefacebook-companies (last visited on May 30, 2022).

[116] Ankit Kumar, WhatsApp's Separate Privacy Policies for Europe and India Raise Concerns, India Today, *available at:*
https://www.indiatoday.in/technology/news/story/whatsapp-s-separate-privacy-policies-for-europe-and-india-raises-concerns-1758888-2021-01-14 (last visited on May 30, 2022).

[117] 2016 SCC OnLine Del 5334.

The Supreme Court stayed the policy and held that "Right to privacy must be respected in every situation. It also directed the appropriate authority to frame effective legal framework for avoiding such breach of privacy."

In the recent WhatsApp case, the personal data of the users who will be operating as a business account will be shared without giving them the chance of choosing to protect their privacy. This has led to a widespread backlash against WhatsApp even though they have announced that they will not misuse any data.

In matter of ***'X' Versus Union of India and Others (2021)***[118], the principal grievance of the petitioner in this case is that her photographs and images that she had posted on her private social media accounts on 'Facebook' and 'Instagram' have been taken without her knowledge or consent and have been unlawfully posted on a pornographic website called 'www.xhamster.com' by an unknown entity called 'Desi Collector' whereby the petitioner's photographs and images have become offensive by association. The queries framed by Hon'ble Delhi High Court were to the following effect:

- Where a party seeks relief from the court to the effect that certain offending or illegal content be removed from the worldwide-web, what directions are required to be passed by a court to make its order implementable and effective; and to which parties are such directions required to be issued;
- What steps are required to be taken by law enforcement agencies to implement such directions issued by a court to ensure that despite court orders/directions offending content does not 'resurface' or remain available on the world-wide-web at the instance of errant parties; and such parties do not succeed in brazenly evading compliance of such orders/directions with impunity.

Hon'ble High Court suggested template directions that should ordinarily be issued and the parties to whom these should be issued are as follows:

The Hon'ble Delhi High Court opined that a fair balance between the obligations and liabilities of the intermediaries and the rights and interests of the aggrieved user/victim would be struck by issuing directions as detailed below, which would be legal, implementable, effective and would enable meaningful compliance of the orders of a court without putting any impossible or untenable burden on intermediaries.

[118] 2021 SCC OnLine Del 1788: (2021) 280 DLT 57

In matter of ***Manohar Lal Sharma Versus Union of India and Others (2021)***[119] (Popularly known as Pegasus Case) the Hon'ble Supreme Court is called upon to examine an allegation of the use of such a modern technology, its utility, need and alleged abuse. The factual position of the present case is as follows:

"In September 2018, Citizen Lab, based out of the University of Toronto, Canada, released a report detailing the software capabilities of a Pegasus spyware developed by an Israeli Technology firm, viz., the NSO Group. The report indicated that individuals from nearly 45 countries were suspected to have been affected. Once the software installed on an individual's device, it has the capacity to access the entire stored data on the device, and has real time access to emails, texts, phone calls, as well as the camera and sound recording capabilities of the device. On 18 July 2021, a consortium of nearly 17 journalistic organizations from around the world, including one Indian organization, released the results of a long investigative effort indicating the alleged use of the Pegasus software on several private individuals. This investigative effort included a list of some 50,000 leaked numbers (out of which 300 numbers belonged to Indians) under surveillance by clients of the NSO Group through the Pegasus software. The above reports resulted in largescale action across the globe. Some of the Writ Petitioners before Hon'ble Supreme Court of India allege to be direct victims of the Pegasus attack, while others are Public Interest Litigants.

Hon'ble Supreme Court while dealing with these petitions made following observations: the entire citizenry is affected by such allegations due to the potential chilling effect; no clear stand taken by the Respondent-Union of India regarding actions taken by it; possibility that some foreign authority, agency or private entity is involved in placing citizens of this country under surveillance.

The Hon'ble Supreme Court constituted a technical committee under the supervision of Justice R.V. Raveendran, former Judge, Supreme Court of India to enquire, investigate and determine:

i. Whether the Pegasus suite of spyware was used on phones or other devices of the citizens of India to access stored data, eavesdrop on conversations, intercept information and/or for any other purposes not explicitly stated herein?

ii. The details of the victims and/or persons affected by such a spyware attack.

[119] 2021 SCC OnLine SC 985.

iii. What steps/actions have been taken by the Respondent-Union of India after reports were published in the year 2019 about hacking of WhatsApp accounts of Indian citizens, using the Pegasus suite of spyware.

iv. Whether any Pegasus suite of spyware was acquired by the Respondent-Union of India, or any State Government, or any central or state agency for use against the citizens of India?

v. If any governmental agency has used the Pegasus suite of spyware on the citizens of this country, under what law, rule, guideline, protocol or lawful procedure was such deployment made?

The Hon'ble Supreme Court of India has directed this committee to make recommendations regarding enactment or amendment to existing law and procedures surrounding surveillance and for securing the improved right to privacy; regarding enhancing and improving the cyber security of the nation and its assets; to ensure prevention of invasion of citizens' right to privacy, otherwise than in accordance with the law, by State and/or non-State entities through such spywares; regarding the establishment of a mechanism for citizens to raise grievances on suspicion of illegal surveillance of their devices; regarding the setting up of a well-equipped independent premier agency to investigate cyber security vulnerabilities, for threat assessment relating to cyberattacks and to investigate instances of cyberattacks in the country.

## 5.10 INDIA'S INTERNATIONAL OBLIGATIONS IN RELATION TO PRIVACY

India is a signatory to the International Covenant on Civil and Political Rights 1966 (ICCPR), Article 17 includes protection of privacy. Treaties are not enforceable under Indian law until they are incorporated into domestic law.[120] However, article 21 of Indian Constitution has to be interpreted consistently with international law.[121] India is not a signatory to the 1st Optional Protocol to the ICCPR, so it is not possible for Indian citizens to make complaints to the UN concerning failures to fully implement Article 17. India is not a party to any of the other significant international data protection agreements. It is not a member of the OECD or of the Asia Pacific Economic

[120] The Constitution of India, Article 253.
[121] *People's Union for Civil Liberties (PUCL) v. The Union of India & Anr.* (1996) IN SC 1637 per Kuldip Singh J.

Cooperation (APEC). The South Asian Association for Regional Cooperation (SAARC), the regional organization of which India is the largest member, does not list human right or privacy among its seven current areas of cooperation.[122]

## 5.11 CONCLUSION

The right to privacy, before ***Puttaswamy case***[123] derived its ambiguous basis from the right to life and personal liberty, as enshrined in Article 21. On 24 August 2017, a Constitutional Bench of nine judges of the Supreme Court of India in ***Justice K.S. Puttaswamy***[124] upheld that Privacy is a Fundamental Right, which is entrenched in Article 21 [Right to Life & Liberty]. The Supreme Court urged the Government to put in place a robust mechanism for data protection. The Court observed that the creation of a regime requires a careful and sensitive balance between individual interests and legitimate concerns of the State. It is legitimate to collect personal data in the public interest, but this information should be protected and used only for the purposes it was collected. Above all, the law must provide for a suitably empowered statutory authority to enforce its promised protection to citizens' data and loss of individual autonomy.

Hon'ble Supreme Court of India in this case further held that Indians have a constitutionally protected fundamental right to privacy that is an intrinsic part of life and liberty under Article 21 and further held that privacy is a natural right that inheres in all natural persons, and that the right may be restricted only by state action that passes each of the following three tests:

- First, such state action must have a legislative mandate;
- Second, it must be pursuing a legitimate state purpose; and
- Third, it must be proportionate i.e., such state action — both in its nature and extent, must be necessary in a democratic society and the action ought to be the least intrusive of the available alternatives to accomplish the ends.

India does not have any specific law for data protection. Statutory protection of privacy can be found in India is scattered across a number of statutes. It had become increasingly evident that the Information Technology Act, 2000 did not have suitable privacy and data protection provisions in the regime of era of social media.

[122] Graham Greenleaf, *Asian Data Privacy Laws* 410 (Oxford University Press, United Kingdom, 2017).
[123] *Supra* note 1.
[124] *Supra* note 1.

Although the Information Technology Act, 2000 attempts to address the issue of protecting privacy rights, it fails to meet the breadth and depth of protection that the EC Directive mandates as it only protects privacy rights from Government action. It is unclear whether such protection extends to private actions. Furthermore, unlike the EC Directive which imposes liability on each participant within the chain of command of the data who failed to protect the sanctity of the data, existing Indian laws only prosecute those individuals who directly violate laws related to computer systems. Companies or individuals are exempted from liability for breaches of data privacy unless such violations were made knowingly. Moreover, unlike the EC Directive which protects against data breaches by limiting data collection and use, the Indian laws do not specify conditions under which data can be collected and used.

In today's global economy, the importance of strong, enforceable, and internationally interoperable data protection standards cannot be underestimated. This is very true for India, as it has sought, and is seeking to position itself as an attractive destination for business and data processing. To help achieve this goal, India sought 'data secure' status from the European Union in 2012 as part of negotiations on the free trade agreement with the region. According to the Data Security Council of India, if India were to receive adequacy, the Indian out- sourcing sector could increase from $20 billion to $50 billion annually. For many years, India has also been seeking membership to the Asia-Pacific Economic Cooperation (APEC).[125]

A rights-oriented data protection legislation is the need of the hour which includes comprehensive surveillance reform prohibiting mass surveillance and institution of a judicial oversight mechanism for targeted surveillance, and which recognises the principle that the state ought to be a model data controller as it deals with its citizens' personal information.

For the privacy judgment to fulfil its true promise, it needs to go beyond spirited dissents to firm, binding judgments that keeps the political executive within clear, limited constitutional boundaries.[126]

[125] David J. Kessler, Sue Ross and Elonnai Hickok, "A Comparative Analysis of Indian Privacy Law and The Asia-Pacific Economic Cooperation Cross-Border Privacy Rules" 26 (1) *National Law School of India Review* 31-32 (2014).
[126]https://www.drishtiias.com/daily-updates/daily-news-editorials/privacy-judgement-and-the-aftermath

1. A comprehensive statute needs to be passed by the Parliament which should cover various aspects including social media, where, as elaborated, statutory law is essential.

2. Information Technology Act, 2000 needs a major revamp with respect to social media to widen the definition of privacy as per the definition in Black's Law Dictionary as the current definition does not capture the essence of privacy.

3. Proper implementation of the judgment of the constitutional bench in the right to privacy case is important.

**One of the hypotheses of the present study was "Inappropriate legislations are hampering protection of privacy rights of social media users".**

**On the basis of the discussion in Chapter IV: Privacy Laws & Social Media: International Perspective and Chapter V: Privacy Laws & Social Media: Indian Perspective, the researcher has reached the conclusion that "Inappropriate legislations are hampering protection of privacy rights of social media users". Hence, the hypothesis is proved.**

# CHAPTER-VI
# DATA ANALYSIS AND INTERPRETATION

# CHAPTER VI
# DATA ANALYSIS AND INTERPRETATION

## 6.1 INTRODUCTION

Social media is not merely a tool for exchanging messages in the digital age, but it has increasingly become a means for information dissemination, interaction, and global participation. Social media has opened a plethora of opportunities for the users, especially for the young people who no longer need a physical space for innovative and initiative action. If social media is used effectively, has the power to harness the potential of the youth and direct them towards civic engagement.

Social media is a fast-growing phenomenon in India, as more and more young Indians are getting access to smartphones and the internet. With 250+ million social network users, India has the second-highest number of social media users in the world. Facebook, YouTube, and WhatsApp dominate the social media space in India. While Instagram is also very popular amongst urban Indian youth.[1]

About two-thirds of Indian youth perceive addiction to social media, loss of privacy, fake news, and cyberbullying as potential risks of social media.[2]

One of the objectives of this study is to examine the awareness of students regarding legal provisions and privacy policies of social media among the students of central universities in Uttar Pradesh. The researcher took this objective in hand to prove/disprove one of the hypotheses "awareness regarding legal provisions and privacy policies of social media among the students of central universities in Uttar Pradesh is not adequate" of the present study. To serve the aforesaid purpose the researcher has divided the study into two parts: Part A and Part B; apart from the Introductory portion. Part A contains the information collected in a form of a questionnaire with 25 questions from students and Part B contains the information collected from Central Universities in Uttar Pradesh through RTI applications with six questions. Data in Part A and Part B has been analysed. The researcher has made efforts

[1] Social Media for Youth and Civic Engagement in India, page 11 (2019) *available at*: https://www.coursehero.com/file/80975786/SOCIAL-MEDIA-REPORTpdf/ (last visited on May 30, 2022).
[2] *Ibid.*

to extract certain findings on the basis of data analysis in order to put their suggestions in resolving issues in social media concerned with the young generation.

### 6.1.1 UTTAR PRADESH AT A GLANCE

**Figure: 6.1 Map of Uttar Pradesh**


*Source: Google Image*

Ruskin Bond while sharing his experiences of his visit to India stated that 'I had been to other countries - in Europe, Asia and the Middle East - but none of them had provided even half as much variety, or so much to see and experience and remember, as this one State in northern India.' While praising the uniqueness of Uttar Pradesh he further stated that 'You can travel from one end of Australia to the other, but everywhere on that vast continent you will find that people dress in the same way, eat the same kind of food, and listen to the same music. This colourless uniformity is

apparent in many other countries of the world, both East and West. But Uttar Pradesh is a world in itself.'[3]

Uttar Pradesh is blessed with a diverse range of natural terrain and cultural diversity. Historical figures such as Buddha, Rama, Krishna, Mahavira, Ashoka, Harsha, Akbar, and Mahatma Gandhi all lived in Uttar Pradesh. Uttar Pradesh's rich and serene expanses of meadows, perennial rivers, dense forests, and fertile soil have contributed several golden chapters to Indian history. Uttar Pradesh, which is dotted with many holy shrines and pilgrim sites and is full of cheerful festivals, plays a vital role in India's education, politics, culture, industry, agriculture, and tourism.

**SOCIAL DEMOGRAPHY -** Uttar Pradesh is a crucial state in the country in terms of population, political awareness, historical and cultural heritage, and the liberation movement. The state is home to 16.17 percent of India's population. Geographically, it ranks fifth after Rajasthan, Madhya Pradesh, Maharashtra, and Andhra Pradesh, with 7.3 percent of India's land area. The state's labour force is 23.7 percent, with farmers accounting for 65.9% and industrial employees accounting for 5.6 percent. According to current rates, its per capita income is Rs. 13,262.[4]

**Table: 6.2 Demographic, Educational, and Political Profile of Uttar Pradesh**

| | |
|---|---|
| Area | 240928 square K.M. |
| No. of districts | 75 |
| Total population (year 2011) | 19,98,12341 |
| Male | 10,44,80510 |
| Female | 9,53,31831 |
| Population growth during 2001-2011 | 33614420 |
| Decline in population rate during 2001-2011 | 20.29% |
| Density of population (per sq. km) | 829 |
| Sex ratio | 912:1000 |
| Lok Sabha Seats | 80 |
| Rajya Sabha Seats | 31 |
| Legislative Assembly Seats | 404 |
| Legislative Council Seats | 100 |
| Overall Literacy Rate | 73% |

[3] Government of Uttar Pradesh Official Website https://up.gov.in/upstate.aspx (last visited on May 30, 2022).
[4] Social Demography *available at*: https://up.gov.in/Social-Demography.pdf (last visited on May 30, 2022).

| | |
|---|---|
| Literacy Rate (Male) | 77.3% |
| Literacy Rate (Female) | 57.2% |

**Source:** https://up.gov.in/Social-Demography.pdf

### 6.1.2 UTTAR PRADESH FROM INFORMATION TECHNOLOGY POINT OF VIEW

Today, information technology plays a significant role in the country. Uttar Pradesh, the country's most populated state and third-largest economy, is North India's IT hub, with a share of software exports second only to Karnataka. As one of the largest contributors to the IT/ITeS sector, the state has continually focused on infrastructure development, human capital development, and effective policy execution in order to provide a favourable environment for the IT-BPM business.

The Department of IT & Electronics (IT & E) established in 1994 with a vision "To use I.T. as a vehicle for economic development of Uttar Pradesh with inclusive growth to create a vibrant society with a high quality of life" is the guiding force for other departments of the state for the usage and deployment of IT for their benefits and benefits of their consumers. The Department of Information Technology and Electronics provides technical assistance to other government departments through the corporations and societies that fall under its jurisdiction. The mission of the state in development of IT infrastructure is to leverage IT as an engine of growth for UP; to transform physical communities into connected communities that can help to realise sustainable economic growth and enhance the quality of life.

The establishment of a 100-acre IT city on a PPP model in Lucknow with a state-of-the-art skill development centre with a capacity of 5,000 students per year is one of the department's significant achievements under policy execution. Another project is the construction of IT parks in Agra, Meerut, Ghaziabad, Kanpur, and Gorakhpur, which is now underway.

More than 20,000 Common Service Delivery outlets, such as Jan Seva Kendra, Lokvani Kendra, and e-Suvidha Kendra, have been established across the state to help citizens with e-Government. These outlets deliver citizen-centric services from various departments electronically to citizens' doorsteps.[5]

[5] http://upite.gov.in/StaticPages/background.aspx (last visited on May 30, 2022).

### 6.1.3 USE OF SNSs/APPS IN UTTAR PRADESH GOVERNMENT

Apart from developing IT infrastructure in the State, numerous departments of the Uttar Pradesh are relying on the services of social networking sites and apps to get connected with citizens. Table 6.3 below showing the department using different SNSs/apps.

**Table 6.3:** Department using SNSs/Apps in Uttar Pradesh Government

| Department | Website | SNSs/Apps |
|---|---|---|
| Agriculture Department | कृषि विभाग, उत्तर प्रदेश, भारत के राज्य सरकार की आधिकारिक वेबसाइट। (upagripardarshi.gov.in) | Facebook, Twitter, YouTube |
| Uttar Pradesh Commercial Tax Department | ::Commercial Tax Department: (up-gst.com) | Facebook, Twitter, YouTube |
| Directorate of Civil Aviation | Directorate of Civil Aviation, Govt of Uttar Pradesh, Lucknow Airport, Lucknow, INDIA (cadup.gov.in) | Facebook, Twitter, Pinterest |
| Department of Dharmarth Karya | धर्मार्थ कार्य विभाग \| उत्तर प्रदेश सरकार (updharmarthkarya.in) | Facebook, Twitter, Google Plus, YouTube, Gmail |
| Chief Electoral Officer, UP | Chief Electoral Officer, Uttar Pradesh (ceouttarpradesh.nic.in) | Facebook, Twitter, YouTube |
| Higher Education Department | उच्च शिक्षा विभाग, उत्तर प्रदेश, भारत के राज्य सरकार के विभाग की आधिकारिक वेबसाइट। (uphed.gov.in) | Facebook, Twitter, Google Plus, YouTube, Google Map |
| Home Department | गृह विभाग, उत्तर प्रदेश (भारत) सरकार की वेबसाइट में आपका स्वागत है (uphome.gov.in) | Facebook, Twitter, Google Plus |
| Department of IT & Electronics | upite.gov.in\| Official Website of Department of IT and Electronics,State Government of Uttar Pradesh, India. | Facebook, YouTube, Twitter |
| NRI Department | Official Website of NRI Department, Government of Uttar Pradesh, India \| UPNRI | Facebook, Twitter, Google Plus, YouTube, Google Map, Gmail |
| Revenue Department | मुख्य पृष्ठ: राजस्व विभाग, उत्तर प्रदेश (up.nic.in) | Facebook, Twitter, Google Plus |
| Public Works Department | :: UPPWD.gov.in \| Official website of Public Works Department,Uttar Pradesh :: | Facebook, Twitter, LinkdIN |
| Rojgar Sangam | Rojgaar Sangam (up.nic.in) | Facebook, Twitter, LinkdIN, YouTube |
| U.P. Police | uppolice.gov.in\| Official Website of Uttar Pradesh Police | Facebook, Twitter, YouTube |

From Table 6.3 it is clear that Facebook, Twitter, LinkedIn, YouTube, Google Plus, Gmail, Pinterest etc. are being used by the different departments of Government of Uttar Pradesh.

## 6.2 HIGHER EDUCATION SYSTEM IN INDIA

Higher education has always occupied a prominent place in Indian history, dating back to the ancient times. Nalanda, Taxila, and Vikramsila universities were renowned centres of higher learning in ancient India, attracting students from all over the country as well as from far away countries such as Korea, China, Myanmar, Sri Lanka, Tibet, and Nepal. India now has one of the world's most extensive higher education systems.[6]

The evidence of present system of higher education is recorded in Mountstuart Elphinstone's minutes of 1823, which emphasized on the need for establishing schools for teaching English and the European science Lord Macaulay pushed for "efforts to make inhabitants of the nation thoroughly proficient English students" in 1835. Sir Charles Wood recommended the creation of a well-articulated educational programme from elementary school to university in 1854. It aimed to promote indigenous education and planned the development of a comprehensive educational policy. Calcutta, Bombay (now Mumbai), and Madras universities were set up in 1857, followed by the University of Allahabad in 1887.[7]

With the Report of the Central Advisory Board of Education on Post-War Educational Development in India, popularly known as the Sargeant Report, efforts were made for the first time in 1944 to design a national system of education in India. The University Grants Committee, which was established in 1945 to oversee the activities of the three Central Universities of Aligarh, Banaras, and Delhi, was suggested in the Report. In 1947, the Committee was tasked with dealing with all of the universities that existed at the time.

The University Education Commission was established in 1948, Dr S Radhakrishnan as a chairman, to "report on Indian university education and propose improvements and expansions that may suit the present and future needs and aspirations of the country". The report recommends that the University Grants Committee be

[6] https://www.ugc.ac.in/page/Genesis.aspx (last visited on May 30, 2022).
[7] *Ibid.*

restructured along the general model of the UK's University Grants Committee, with a full-time chairman and other members.

In 1952, the Union government decided that all matters relating to the allocation of grant-in-aid from public funds to central universities and other universities and institutions of higher education could be referred to the Commission on University Grants. UGC was formally established in November 1956 by an Act of Parliament to coordinate, define and maintain the standards of university education in India. The head office of the UGC is located at Bahadur Shah Zafar Marg in New Delhi.

The revolution in Internet, social media, and information technology has had a big impact on the higher education system in India and the world as a whole. Due to social media sites like Google Meet, Facebook, and ZOOM, people are more likely to communicate and meet new people. During the Covid-19 pandemic, both new opportunities and serious threats arose for learners. While the opportunities offered new ways of learning, as well as posed a serious threat to the rights of individuals, especially the right to privacy.

### 6.2.1 HIGHER EDUCATION SYSTEM IN UTTAR PRADESH

Uttar Pradesh has a large number of academic and research institutes. These institutes are either run by the State Government, the Central Government, or are private owned institutions. The state has two IITs – at Kanpur and Varanasi, an IIM at Lucknow, many state universities, an NIT and an IIIT at Allahabad. A good number of State and Central Government universities are founded in Uttar Pradesh to provide Higher Education in various disciplines.

The Rajiv Gandhi Institute of Petroleum Technology: The Ministry of Petroleum and Natural Gas, Government of India set up the institute at Jais, Rae Bareli district, Uttar Pradesh. RGIPT has been accorded Institute of National Importance. With the status of a deemed university, the institute awards degrees in its own right. RGIPT is co-promoted as an energy domain-specific institute by six oil public sector units (ONGC, IOCL, OIL, GAIL, BPCL and HPCL) in association with the Oil Industry Development Board (OIDB). The institute is associated with leading International Universities/Institutions specializing in the domain of Petroleum Technology.

Apart from above mentioned institutes of higher learning, in Uttar Pradesh, a range of Government Degree College has been set up by the Government of Uttar

Pradesh for providing Higher Education to scholars who are interested in different disciplines.[8]

Table 6.4 shows a list of some of the universities in Uttar Pradesh. Table 6.4 shows the trend among the universities adopting privacy policies in order to respect the right to privacy of the individuals, whereas some of the universities are not taking privacy concerns seriously.

**Table 6.4: STATE UNIVERSITIES IN UTTAR PRADESH**

| University Name | Year of Establishment | Place | Website | Privacy Policy adopted |
|---|---|---|---|---|
| Uttar Pradesh Rajshri Tandon Open University | 1999 | Prayagraj | http://www.uprtou.ac.in/ | - |
| University of Lucknow | 1921 | Lucknow | University of Lucknow (lkouniv.ac.in) | Yes |
| Chhatrapati Shahu Ji Maharaj University | 1965 | Kanpur Nagar | www.csjmu.ac.in | Yes |
| Dr. Ram Manohar Lohia Awadh University | 1975 | Ayodhya | www.rmlau.ac.in | - |
| Chaudhary Charan Singh University | 1965 | Merrut | www.ccsuniversity.ac.in | - |
| Mahatma Gandhi Kashi Vidyapith | 1974 | Varanasi | www.mgkvp.ac.in | Yes |
| Sampurnanand Sanskrit University | 1958 | Varanasi | www.ssvv.ac.in | - |
| Bundelkhand University | 1975 | Jhansi | www.bujhansi.ac.in | - |
| Mahatma Jyotiba Phule Rohilkhand University | 1975 | Bareilly | www.mjpru.ac.in | - |
| Dr. Bhimrao Ambedkar Agra University | 1927 | Agra | www.dbrau.ac.in | - |

**Source:** https://uphed.gov.in/UniversityDetail.aspx?value=STATE (last visited on May 30, 2022).

[8] https://en.wikipedia.org/wiki/Education_in_Uttar_Pradesh (last visited on May 30, 2022).

## 6.3 CENTRAL UNIVERSITIES IN UTTAR PRADESH

There are 54 Central Universities in India[9]. Out of these universities six central universities are imparting higher education to the students in Uttar Pradesh.

### 6.3.1 ALIGARH MUSLIM UNIVERSITY, ALIGARH

Aligarh is one of the districts of Uttar Pradesh, in India. The distance of Aligarh is about 90 miles (140 km) from New Delhi. Before the 18th century, Aligarh was known by the name of Kol or Koil. It is mostly known as a university town where the famous Aligarh Muslim University is located. In 1875, Sir Syed Ahmed Khan established the Muhammadan Anglo Oriental College in Aligarh, followed the pattern of Oxford and Cambridge universities that he had visited on a trip to England. This later became Aligarh Muslim University in 1920.[10]

**Figure:** 6.5 Aligarh Muslim University, Aligarh

*Source:* Google Image

This university spread over 467.6 hectares in the city of Aligarh, Uttar Pradesh. The university has kept its door open to the members of all communities and from all corners of the country and the world since inception.

The university offers more than 300 courses in the traditional and modern branches of education. Students from all states in India and from different countries, including Africa, West Asia and Southeast Asia are enrolled here. In some courses,

[9] https://www.ugc.ac.in/oldpdf/Consolidated_CENTRAL_UNIVERSITIES_List.pdf (last visited on May 30, 2022).
[10] Official Website of Aligarh Muslim University: https://aligarh.nic.in/ (last visited on May 30, 2022).

special seats are reserved to encourage students from SAARC and Commonwealth Countries. The University is open to all irrespective of caste, creed, religion or gender.

The University has excellent infrastructures including 13 faculties comprising 117 teaching departments, 3 academies and 21 centres and institutes. The University provides residential quarters to most of the staff and students. There are 19 halls of residence for students with 80 hostels.[11]

Apart from the conventional Undergraduate and Postgraduate courses in Social Sciences, Sciences and Humanities, the University keeps pace with the nation's growth by offering facilities for specialized learning in areas of technical, vocational and interdisciplinary studies.[12]

The University has opened three new centres of study outside Aligarh at Murshidabad, West Bengal state, at Mallapurum, Kerala state and at Kishanganj, Bihar State.

One primary, seven high schools (one of which is for students with visual impairments), and two senior secondary schools for both boys and girls are all maintained by the university. Additionally, the university provides courses in Western, Oriental, and Indian languages. English is used as the primary language of instruction at the university.

**MAULANA AZAD LIBRARY** - Maulana Azad Library is the Central Library of the Aligarh Muslim University which is famous for its invaluable collections of manuscripts, rare books and artifacts. The library meets the needs of its students, academics and research scholars with a wide range of library services provided by more than 110 college and departmental libraries including Engineering College Library, Medical College Library, Social Science Cyber Library and Ajmal Khan Tibbiya College Library.[13]

Maulana Azad Library is providing access to Grammarly, an English writing assistance tool for faculty members and research scholars .

[11] http://www.amu.ac.in (last visited on May 30, 2022).
[12] *Ibid.*
[13] https://amu.ac.in/libraries/maulana-azad-library (last visited on May 30, 2022).

Maulana Azad Library provides remote access to the subscribed e-resources like e-books, e-contents, journal articles and databases etc. from outside the campus through "OpenAthens" remote login solution to faculty members and research scholars of the university.

Maulana Azad Library has subscribed 'Turnitin' a plagiarism detection tool. Faculty members and research scholars of university can access it to check plagiarism in research articles, dissertation, book chapters, reports etc. by their own.[14]

**CENTRE FOR DISTANCE AND ONLINE EDUCATION** - The Centre for Distance and Online Education (CDOE) is an integral part of the University. Adopting flexible and innovative methods of education to ensure 'independent learning' to anyone, anytime and anywhere, the Centre offers programmes of the study that are customized to meet the learning requirements of knowledge seekers as well as to ensure that they learn at their own pace and convenience.

**IT HELP DESK -** IT Help Desk of Prof. M. N. Farooqui Computer Centre is a technology adoption support facility for Campus Users of AMU, it facilitates answering of technical queries and also offers Remote Support related to central IT Services of University for all registered Users.

### 6.3.2 BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY, LUCKNOW

Lucknow, popularly known as the City of Nawabs is the capital city of Uttar Pradesh and it has always been a multicultural city. Courtly manners, beautiful gardens, poetry, music, and fine cuisine patronized by the Persian-loving Shia Nawabs of the city are well known amongst Indians and students of South Asian culture and history.

**Figure**: **6.6** Babasaheb Bhimrao Ambedkar University, Lucknow

*Source:* Google Image

[14] https://amu.ac.in/libraries/maulana-azad-library (last visited on May 30, 2022).

The Babasaheb Bhimrao Ambedkar University situated in Vidya Vihar, Raebareli road, Lucknow. The university was established in 1996. The University distinguishes itself as a socially responsible learning community of high-quality scholarship and academic rigor sustained by social justice and equity principles for which Babasaheb Bhimrao Ambedkar worked during his lifetime. 50 percent seats of the all courses are reserved for the student of Schedule Caste and Schedule Tribes in the university. Now with the government directives university also offers 10 percent seats reserved for the Economically Weaker Section[15].

This University offers diverse programs in the disciplines of – Humanities and Sciences, Engineering, Agriculture, Biotechnology, Business, Law, Human Rights, Education and Environmental Sciences. University offers more than 99 courses that includes Diploma/integrated PG Programmes/UG/PG/M.Phil. and Ph.D. at its main campus and satellite campus at Amethi.[16]

**GAUTAM BUDDHA CENTRAL LIBRARY -** The Central Library of Babasaheb Bhimrao Ambedkar University has named as Gautam Buddha Central Library after the name of Lord Buddha. The library has been adapting new technologies strategically for providing web-based information services to the library users with the dynamic nature of ICT. The library is member of 'E-ShodhSindhu' National Consortium for Higher Education Electronic Resources of INFLIBNET (Information and Library Network), Gandhinagar. *Inter alia* different sections, cyber section has the strength of 50 computers, but presently, a total of 25+ computers with the facility of access to the internet are functioning. The library has Wi-Fi enabled access to the Internet where the users access the e-resources. The students are allowed to use their Laptops and Tablets here.

The library partially automated by using an Open-Source Integrated Library Management Software (ILMS) namely KOHA. Automation work in several sections such as Circulation, Technical, Thesis, Periodical section have started with the help of KOHA. All the Bibliographic data of Books/Theses/Dissertations/Periodicals have migrated on ILMS (KOHA).

[15] www.bbau.ac.in (last visited on May 30, 2022).
[16] *Ibid.*

**UNIVERSITY COMPUTER CENTRE -** The University Computer Centre was established in year 2008. Centre caters the overall ICT (Information and Communication Technology) need of the entire University. The centre has been helping University in Computerization of various Sections, expanding the University Networks to reach various buildings, procurement, automation, development of various tools and utility software and maintenance of university Website, Establishment and Growth of University computer centre Training and other Various Activities since the inception.[17]

The computer centre at BBAU assists in Live coverage of all major events including video conferencing & teleconferencing; provides technical assistance during the Convocations/ Conferences / Seminars & other University functions etc.; manages the WebEx license for online classes and meetings for entire University; assist various departments of the University in computerizing their activities.

### 6.3.3 BANARAS HINDU UNIVERSITY, VARANASI

Varanasi is one of the oldest cities in the world. For nearly three thousand years, the city has been a hub of scholarship and civilisation. With Sarnath, the place where Buddha preached his first sermon after enlightenment. Here, for millennia, there has been a flourishing of knowledge, philosophy, culture, devotion to Gods, and Indian arts and crafts. Varanasi, which is also a Jains' pilgrimage site, is thought to be the birthplace of Parsvanath, the twenty-third Tirthankar. Varanasi has long been a fantastic hub for learning. Sanskrit, yoga, the Hindi language, and spiritualism are all promoted in Varanasi.[18]

**Figure: 6.7** Banaras Hindu University, Varanasi

*Source:* Google Image

[17] *Ibid.*
[18] https://varanasi.nic.in/about-district/ (last visited on May 30, 2022).

Banaras Hindu University (BHU) is one of the famous universities in Uttar Pradesh. As name conveys, the university is situated in Varanasi. The history of Banaras Hindu University starts with the establishment of Central Hindu College of Varanasi, envisioned as a Hindu university in April 1911 by Annie Wood Besant and Pandit Madan Mohan Malaviya. BHU starts functioning on 1 October 1917, with the Central Hindu College as its first constituent college. It is one of the largest residential universities in Asia. The university has more than 128 independent teaching departments; several of its colleges—including science, linguistics, law, engineering (IIT - BHU) and medicine (IMS-BHU) are ranked amongst the best in India. The university's total enrolment including international students stands at just over 15,000. Over 15,000 people are enrolled in the university overall, including international students. It is the only college in India to have an IIT on its campus (IIT BHU).[19]

**CENTRAL LIBRARY** - Banaras Hindu University Library System consists of 3 Institute Libraries, 8 Faculty Libraries, 25 Departmental Libraries, with a total collection of over 13 lakh volumes to serve the students, faculty members, researchers, technical staff of fourteen faculties consisting of 126 subject departments of the university.

**COMPUTER CENTRE -** The Computer Center offers computing resources to the campus community and assists researchers in analysing their research data. It expands the university's Internet capabilities, permits World Wide Web and email access, and gives scientific and technology students access to lab space. The BHU website and Web servers are maintained by Computer Center. From their offices, academic units, and hostels, users can access the computer center's computing capabilities. All academics, staff, and students have access to a login to use the Internet.[20]

### 6.3.4 RAJIV GANDHI NATIONAL AVIATION UNIVERSITY, RAEBARELI

The district of Raebareli, created by the British in 1858, is named after its headquarters town. It is believed that town was founded by the Bhars and was known as Bharauli or Barauli which in course of time got corrupted into Bareli. It is also said that the prefix, Rae, represents Rae, the common title of the Kayasths who were masters

[19] https://en.wikipedia.org/wiki/Education_in_Uttar_Pradesh (last visited on May 30, 2022).
[20] https://bhu.ac.in/ccbhu/ (last visited on May 30, 2022).

of the town for a considerable period of time. Major Government Industrial Units in Raebareli are N.T.P.C. at Unchahar, Rail Coach Factory at Lalganj, Indian Telephone Industry.[21]

**Figure: 6.8** Rajiv Gandhi National Aviation University, Raebareli


*Source:* Google Image

The Rajiv Gandhi National Aviation University (RGNAU) was established by an Act of Parliament known as the Rajiv Gandhi National Aviation University Act, 2013 at Fursatganj Raebareli, Dist. Amethi, Uttar Pradesh. The university is a premier institution of higher learning providing cutting edge and critical research to enhance the aviation industry in India. Course including Diploma, Degree, and Post-Graduation in the field of civil aviation are run by the university. At the same time collaborations with the leading international universities/ institutions in the aviation domain, are being forged towards proffering global knowledge that is customized to local requirements.[22]

The objective of Rajiv Gandhi National Aviation University is to facilitate and promote aviation studies, teaching, training, research and by extension work in conjunction with the industry to achieve excellence in operations and management of all the sub-sectors within the aviation industry.[23]

[21] https://raebareli.nic.in/about-district/ (last visited on May 30, 2022).
[22] https://rgnau.ac.in/en/about-us (last visited on May 30, 2022).
[23] *Ibid.*

### 6.3.5 RANI LAKSHMI BAI AGRICULTURAL CENTRAL UNIVERSITY, JHANSI

Jhansi district is one of the districts of Uttar Pradesh state in northern India. Jhansi city is a symbol of bravery, courage and self-respect.

**Figure 6.9:** Rani Lakshmi Bai Agricultural Central University, Jhansi


*Source:* Google Image

The Rani Lakshmi Bai Central Agricultural University was established in 2014 under Department of Agricultural Research and Education (DARE). This University was named in the memory of great freedom fighter known as warrior queen of Jhansi Late Rani Lakshmi Bai who sacrificed her life to make India free from the Britishers rule. Like other Agricultural Universities, Central Agricultural University, Jhansi has the key objectives to impart education in different branches of agriculture and allied sciences.[24]

### 6.3.6 UNIVERSITY OF ALLAHABAD, PRAYAGRAJ

Prayagraj is one of the oldest cities in Uttar Pradesh, situated at the confluence of three rivers- Ganga, Yamuna and the invisible Saraswati. The meeting point of confluence of three rivers is known as Triveni.

This city had been the heart of the Indian Freedom Movement against the British rule. Prayagraj has provided the largest number of prime ministers of post-independence India - Pt. Jawahar Lal Nehru, Lal Bahadur Shastri, Indira Gandhi, Rajiv Gandhi, V.P. Singh. Former Prime Minister Chandra Shekhar had been student of Allahabad university.

[24] http://www.rlbcau.ac.in/about_rlbcau.php (last visited on May 30, 2022).

Prayagraj is known as an Administrative and Educational city. High Court of Uttar Pradesh, Auditor General of Uttar Pradesh, Principal Controller of Defence Accounts (Pension) PCDA, Uttar Pradesh Madhymik Shiksha Prishad ( UP BOARD ) office, Police HeadQtrs are situated in Prayagraj. Moti Lal Nehru Regional Engineering College (MNREC), Medical and Agriculture College, Indian Institute of Information Technology (IIIT), University of Allahabad are most prominent education institutions in Prayagraj.

From the days of civilization Prayagraj has been seat of learning, wisdom and writing. It is the most vibrant politically spiritually conscious and spiritually awakened city of India.[25]

**Figure: 6.10** University of Allahabad, Prayagraj

*Source:* Google Image

**University of Allahabad** established on 23rd September 1887, always occupied a prominent place among the Universities of India for over a century. It is the fourth oldest University of India after Calcutta, Bombay and Madras University. The credit for conceiving a large Central College in Prayagraj eventually to develop into a university, goes to Sir William Muir, Lt. Governor of United Provinces.

From the beginning the University has been concerned about women's education. It purchased houses for a women's Hostel and College at the cost of Rs. 66,286 and other buildings adjoining the College. Ever since the inception of the Muir Central College in 1873, efforts were constantly made to accommodate students coming from distant places.[26]

[25] https://prayagraj.nic.in/history/ (last visited on May 30, 2022).
[26] https://www.allduniv.ac.in/about-uoa/about-university1 (last visited on May 30, 2022).

**CENTRAL LIBRARY -** The University Library was started in 1916 to cater the needs of the students, research scholars, and teachers of the University. In 1946-47, Dr.S.R. Ranganathan, father of library science in India, was invited to suggest ways and means of improving the library. He submitted the development plan in March 1947. A special committee was constituted to review the library development plan submitted by Dr. Ranganathan. The committee recommended for erection of a new building designed in accordance with the modern library practice. The present library building is more spacious and has potential for further expansion.[27]

**COMPUTER CENTRE -** The UGC has been helping Universities and Colleges through several general as well as specific schemes to keep pace with the developments in the Information and Communication Technologies (ICT). This centre was conceived sometimes in 1983-84 to meet out the academic needs of the University and was formally established on 26th January, 1987 with the grant-in-aid from the University Grants Commission (U.G.C.), New Delhi. The Objective of setting up a Computer Centre as a Central facility is for the growth and development of teaching, research, other related activities in addition to the work relating to the administration, finance, examination, admission of the University, etc.[28]

[27] https://www.allduniv.ac.in/about-uoa/about-university1 (last visited on May 30, 2022).
[28] *Ibid.*

## 6.4 TOOL AND TECHNIQUES USED IN DATA ANALYSIS AND INTERPRETATION

### 6.4.1 STATISTICAL TOOL

The researcher has used IBM SPSS Statistics Version 21 for analysis of data. SPSS is a statistical software developed by IBM for data management, advanced analytics, multivariate analysis, business intelligence and criminal investigation. SPSS is a widely used program for statistical analysis in social science. It is also used by market researchers, health researchers, survey companies, government, education researchers, marketing organizations, data miners, and others. SPSS was released in its first version in 1968 as the Statistical Package for the Social Sciences (SPSS).[29]

### 6.4.2 DURATION OF DATA COLLECTION

The researcher collected data from students of six central universities in Uttar Pradesh during November, 2021 to February, 2022. The structure questionnaire with twenty-five (25) questions was used to collect data from the students of six central universities in Uttar Pradesh. Total 600 sample size (100 from each university) was taken from six central universities. The sixteen questions were of single response and nine questions were of multiple response.

**Table 6.11:** Types of Questions

| Type of Questions | Number | Questions Numbers |
|---|---|---|
| **Single Response** | 16 | 1, 2, 3, 4, 6, 13, 14, 15, 16, 17, 18, 20, 21, 22, 24, 25 |
| **Multiple Response** | 9 | 5, 7, 8, 9, 10, 11, 12, 19, 23 |

### 6.4.3 STATISTICAL KEY WORDS USED

The researcher feels it appropriate to explain certain key elements used in statistics in order to enhance the readability of the writing. Some of the statistical key words are as follows:

[29] https://en.wikipedia.org/wiki/SPSS (last visited on May 30, 2022).

**Multiple Response** - Multiple response refers to the situation when participants are allowed to select more than one option for a question.[30] Multiple-response questions are quite common in all fields of research, including marketing, education and social sciences as prominent examples.[31]

**Dichotomies:** Use if a single numeric value was used across all of the variables to indicate if the category was "present".

**Missing Values** – Missing Values defines specified data values as user-missing. Missing values could be of two types. One category of missing data is: which has been refused to answer by respondents and another category of missing values are because of the question didn't apply to that respondent. Missing values has been included in data analysis and interpretation by the researcher.

The researcher took the help of following Figure 6.12 $Fruit Frequencies while data analysis and interpretation of multiple response questions as below:

**Figure 6.12:** $ Fruit Frequencies

| | | Responses | | Percent of Cases |
|---|---|---|---|---|
| | | N | Percent | |
| $ Fruit Frequencies [a] | Apples | 9 | 37.5% | 90.0% |
| | Oranges | 5 | 20.8% | 50.0% |
| | Pears | 5 | 20.8% | 50.0% |
| | Bananas | 5 | 20.8% | 50.0% |
| Total | | 24 | 100.0% | 240.0% |

a. Dichotomy group tabulated at value 1.

The above Figure 6.12 $Fruit Frequencies shows that ten people bought 24 pieces of fruit. Nine pieces of fruit were apples – (9/24*100) 37.5% of the fruit. Nine out of ten people bought apples - (9/10*100) 90% of the people. So, the difference is the denominator. What makes this table special is that what the researcher usually cares about is the people with multiple responses.

**DIFFERENT BETWEEN % OF RESPONSES AND % OF CASES**

- % of **responses** indicates what % of the total responses were in each.
- % of **cases** indicates what % of cases mentioned each category.

[30] https://www.academia.edu/13232497/Multiple_Responses_Analysis_using_SPSS_Dichotomies_Method_A_Beginner_s_Guide (last visited on May 30, 2022).

[31] https://statistika.vse.cz/konference/amse/PDF/Plasil+Vlach.pdf (last visited on May 30, 2022).

## 6.5 PART A: ANALYSIS AND INTERPRETATION OF DATA COLLECTED FROM STUDENTS

In this part the researcher has analysed and interpreted data collected from students of six central universities to know their awareness level about legal provisions and privacy policies of social media. The researcher has analysed and interpreted data question wise.

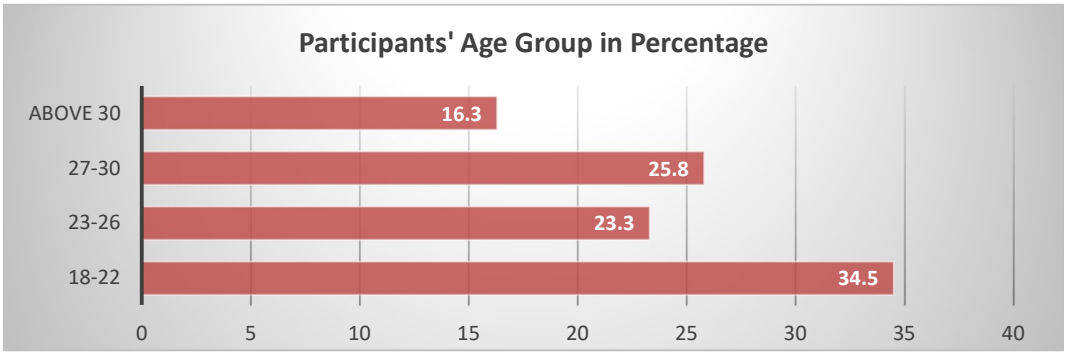
### Q.1. Age Group

Table 6.13 and Figure 6.14 show the participation of respondents age wise. For survey purposes respondents were categorized in four age groups i.e. 18-22, 23-26, 27-30 and above 30. The participation percentage of 18-22 age group is 34.5 % (207 out of 600), the percentage of 23-26 age group is 23.3 % (140 out of 600), the percentage of 27-30 age group is 25.8 % (155 out of 600) and finally the percentage of last age group i.e. above 30 is 16.3 % (98 out of 600). From Table 6.13 and Figure 6.14 it is clear that maximum participation is from the 18-22 age group i.e. 34.5 % (207 out of 600) while as minimum representation is from the age group above 30 is 16.3 % (98 out of 600).

**Table 6.13:** Age Group

| | Age Group | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| **Valid** | **18-22** | 207 | 34.5 | 34.5 | 34.5 |
| | **23-26** | 140 | 23.3 | 23.3 | 57.8 |
| | **27-30** | 155 | 25.8 | 25.8 | 83.7 |
| | **Above 30** | 98 | 16.3 | 16.3 | 100 |
| | **Total** | 600 | 100 | 100 | |

**Figure 6.14:** Age-wise Participation of Respondents



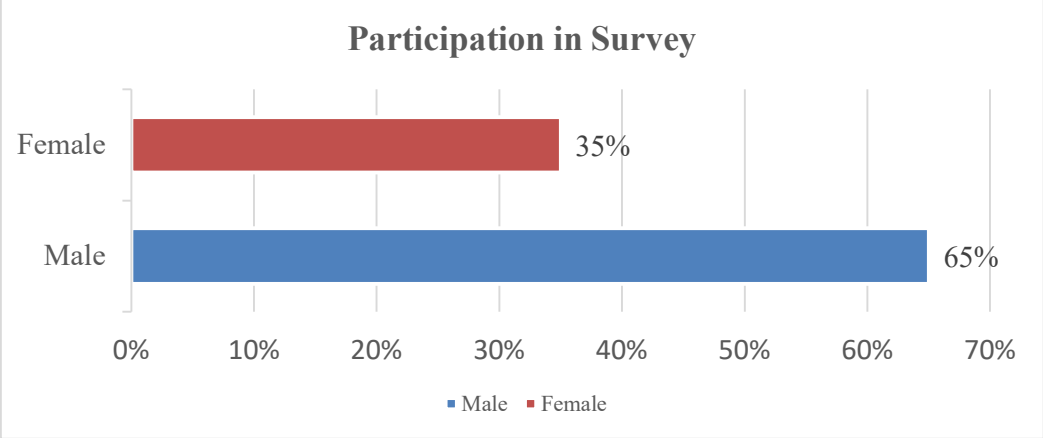
**Q.2. Gender**

Table 6.15 and Figure 6.16 show the gender wise participation of respondents. The table 6.15 and figure 6.16 depict that male's participation is 65% (390 out of 600) while as female's participation is 35% (210 out of 600). Thus, the participation of males is greater than females.

**Table 6.15:** Gender

| Gender | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Male | 390 | 65.0 | 65.0 | 65.0 |
| | Female | 210 | 35.0 | 35.0 | 100.0 |
| | Total | 600 | 100.0 | 100.0 | |

**Figure 6.16:** Gender-wise participation in survey



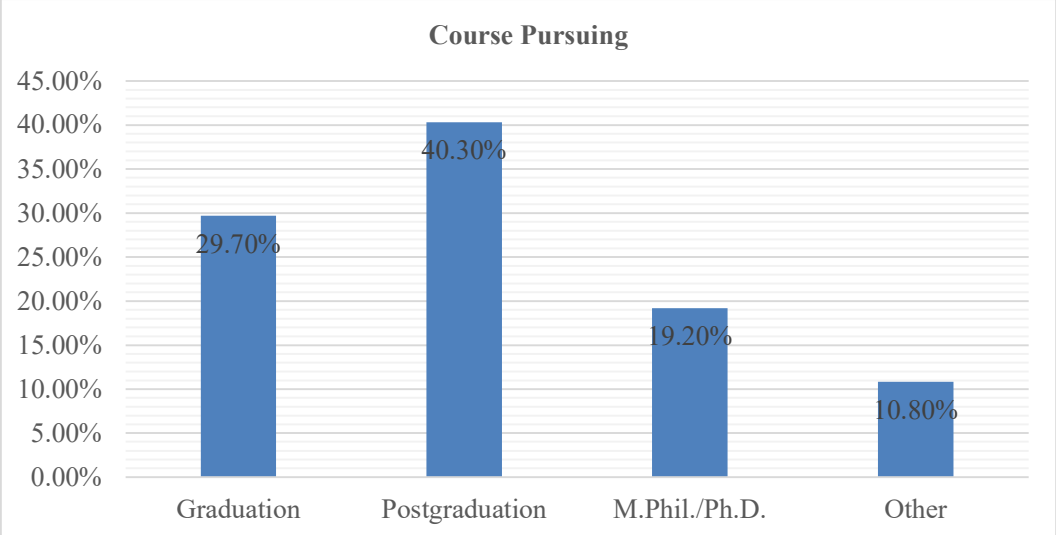
## Q.3. Level of Course Pursuing

Table 6.17 and Figure 6.18 depict course wise representation of respondents in the survey. The table 6.17 and Figure 6.18 show that 29.7 % (176 out of 600) are pursuing graduation, 40.3 % (239 out of 600) are pursuing post-graduation, 19.2 % (114 out of 600) are pursuing M.Phil./Ph.D. while 10.8 % are pursuing other courses like diploma while 1.2 % (7 out of 600) did not respond to this question. Hence, from Table 6.17 and Figure 6.18 it is clear that maximum participation course wise is from the students pursuing post-graduation while minimum participation is from the students pursuing other courses including diploma.

**Table 6.17:** Level of Courses Pursuing by the Respondents

| Course | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | **Graduation** | 176 | 29.3 | 29.7 | 29.7 |
| | **Postgraduation** | 239 | 39.8 | 40.3 | 70.0 |
| | **M.Phil./Ph.D.** | 114 | 19.0 | 19.2 | 89.2 |
| | **Other** | 64 | 10.7 | 10.8 | 100.0 |
| | **Total** | 593 | 98.8 | 100.0 | |
| **Missing** | **System** | 7 | 1.2 | | |
| **Total** | | **600** | **100.0** | | |

**Figure 6.18:** Course Pursuing by the Respondents



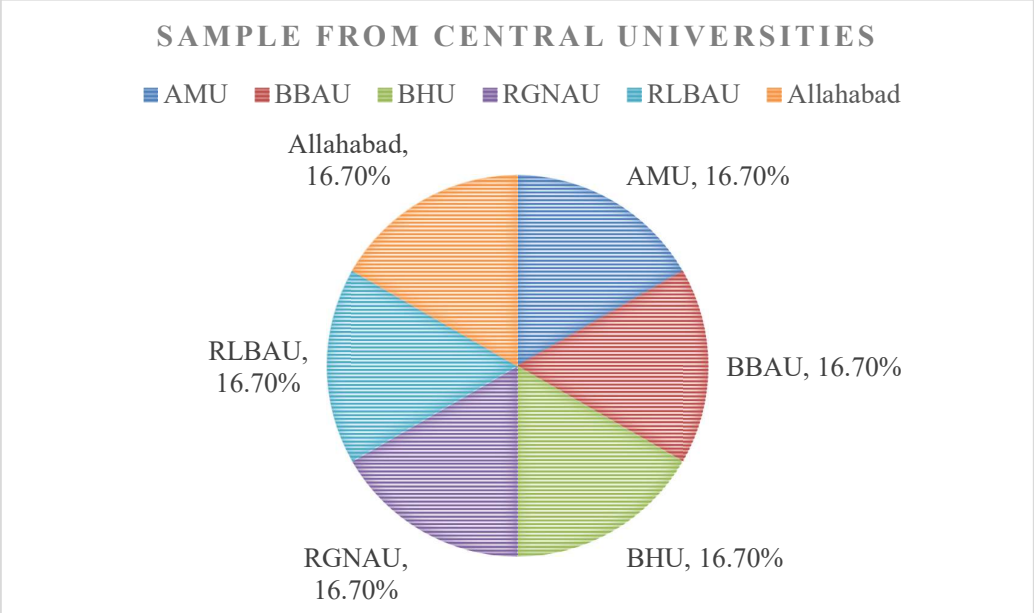
**Q.4. To which university do you belong?**

Table 6.19 and Figure 6.20 provide information regarding samples taken from six central universities – Aligarh Muslim University (AMU) situated in Aligarh, Babasaheb Bhimrao Ambedkar University (BBAU) situated in Lucknow, Banaras Hindu University BHU situated in Varanasi, Rajiv Gandhi National Aviation University (RGNAU) situated in Raebareli, Rani Laxmi Bai Agriculture University (RLBAU) situated in Jhansi and University of Allahabad (UA) situated in Allahabad. 100 samples (16.7%) from each university; thus total 600 samples have been taken in survey for the study.

**Table 6.19:** Students Representation from Each University

| University | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | **AMU** | 100 | 16.7 | 16.7 | 16.7 |
| | **BBAU** | 100 | 16.7 | 16.7 | 33.3 |
| | **BHU** | 100 | 16.7 | 16.7 | 50.0 |
| | **RGNAU** | 100 | 16.7 | 16.7 | 66.7 |
| | **RLBAU** | 100 | 16.7 | 16.7 | 83.3 |
| | **UA** | 100 | 16.7 | 16.7 | 100.0 |
| | **Total** | **600** | **100.0** | **100.0** | |

**Figure 6.20:** Representation of Students from Universities



**Q.5. Which social networking sites (SNSs) /apps do you use?**

Table 6.21 shows that 100% (600 out of 600) respondents responded to this question.

**Table 6.21:** Case Summary of $SNSUsed

| | Cases | | | | | |
|---|---|---|---|---|---|---|
| | Valid | | Missing | | Total | |
| | N | Percent | N | Percent | N | Percent |
| $SNSUsed[a] | 600 | 100.0% | 0 | 0.0% | 600 | 100.0% |

a. Dichotomy group tabulated at value 1

Table 6.22 shows that the researcher received 3221 responses in total. The highest response is 540 in terms of WhatsApp, which suggests that WhatsApp is the first choice of social media users; this total represents 16.8% of total response given (540/3231), but 90.5% of the cases (540/600). YouTube is used by 15.0% of respondents given (482/3221), but 80.7% of the cases (482/600). Facebook is used by 14.1% of total responses given (455/3221) but 76.2% of the cases (455/600). Thus, YouTube is the second choice and Facebook is the third choice of the respondents.

**Table 6.22:** Percentage of Cases of $SNSUsed

| | | Responses | | Percent of Cases |
|---|---|---|---|---|
| | | N | Percent | |
| **$SNSUsed[a]** | **Facebook** | **455** | **14.1%** | **76.2%** |
| | **Instagram** | 380 | 11.8% | 63.7% |
| | **WhatsApp** | **540** | **16.8%** | **90.5%** |
| | **Google** | 454 | 14.1% | 76.0% |
| | **YouTube** | **482** | **15.0%** | **80.7%** |
| | **Google Pay** | 265 | 8.2% | 44.4% |
| | **Twitter** | 155 | 4.8% | 26.0% |
| | **Wikipedia** | 144 | 4.5% | 24.1% |
| | **LinkedIn** | 77 | 2.4% | 12.9% |
| | **Telegram** | 238 | 7.4% | 39.9% |
| | **Others** | 31 | 1.0% | 5.2% |
| **Total** | | **3221** | **100.0%** | **539.5%** |

a. Dichotomy group tabulated at value 1.

**Q.6. Does your university permit you to use social networking sites in your cyber library /computer lab?**

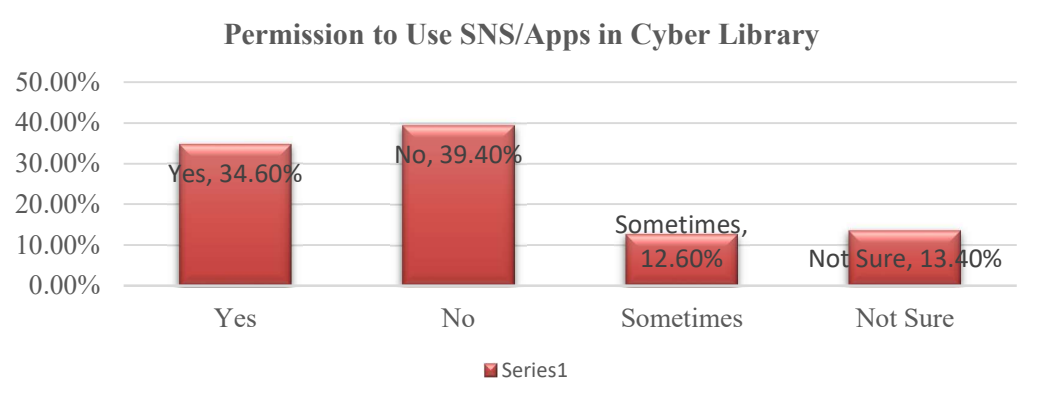
UN Volunteers India and Ministry of Youth Affairs' 2019 Report titled as 'Social Media for Youth and Civic Engagement in India' stated that "Proportion of social media youth users across the states of India, has positive correlation with the State Human Development Index". Researcher has tried to know to what extent universities allow its students to use social networking sites/apps in their cyber libraries through question no. 6 as stated above.

In response to this question as shown below in Table 6.23 and Figure 6.24, 34.60% (204 out of 600) respondents replied positively while 39.4% (232 out of 600) respondents replied negatively. 12.6% (74 out of 600) respondents reply that sometimes they are allowed to use social networking sites/apps, while as 13.4% (79 out of 600) are not sure whether university allow to use SNSs/Apps in its cyber library and 1.8% (11 out of 600) respondents did not respond to this question.

**Table 6.23:** Use of SNS in University's Library

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| **Valid** | **Yes** | 204 | 34.0 | 34.6 | 34.6 |
| | **No** | 232 | 38.7 | 39.4 | 74.0 |
| | **Sometimes** | 74 | 12.3 | 12.6 | 86.6 |
| | **Not Sure** | 79 | 13.2 | 13.4 | 100.0 |
| | **Missing** | 11 | 1.8 | | |
| **Total** | | **600** | **100.0** | | |

**Figure 6.24:** Permission to Use SNS/Apps in Cyber Library



**Q.7. What do you normally post in social media sites / Apps?**

Social Networking Sites/Apps facilitate users to share information in the form of text messages, images, videos, links and other forms. Through the above stated question researcher has tried to know in what form respondents share information with others. Table 6.25 shows that 98.0% (588 out of 600) respondents responded to this question while 2.0% (12) respondents did not respond to this question.

**Table 6.25:** Case Summary of $Posts

| | Cases | | | | | |
|---|---|---|---|---|---|---|
| | Valid | | Missing | | Total | |
| | N | Percent | N | Percent | N | Percent |
| **$Posts[a]** | 588 | 98.0% | 12 | 2.0% | 600 | 100.0% |

a. Dichotomy group tabulated at value 1

**Table 6.26:** Percentage of Cases of $Posts

| | | Responses | | Percent of Cases |
|---|---|---|---|---|
| | | N | Percent | |
| **$Posts[a]** | **Text Messages** | 470 | 34.0% | 79.9% |
| | **Images** | 417 | 30.2% | 70.9% |
| | **Videos** | 247 | 17.9% | 42.0% |
| | **Links** | 179 | 12.9% | 30.4% |
| | **Others** | 70 | 5.1% | 11.9% |
| **Total** | | 1383 | 100.0% | 235.2% |

a. Dichotomy group tabulated at value 1.

Table 6.26 shows that 470 respondents communicate in the form of text messages with others; this total represents 34.0% of total response given (470/1383), but 79.9% of the cases (470/588). 417 responses suggest communication in the form of images; this represents 30.2% of total response given (417/1383), but 70.9% of the cases (417/588). Table further shows that 247 respondents communicate in the form of videos with others; this total represents 17.90% of total response given (247/1383), but 42% of the cases (247/588). 179 responses suggest communication in form of links; this represents 12% of total response given (179/1383), but 30.4% of the cases (179/588). 70 responses suggest that respondents use other forms to communicate; 5.1% of total response but 11.9% of the cases.

**Q. 8. For what purpose do you use social media?**

Social media has as a huge participation from the millennials across the world. In India, social media is a fast-growing phenomenon as more and more people, especially youth, are getting connected with increased penetration of smartphones and internet. The youth in India are excessively dependent on social media be it for communication, education, entertainment, shopping, finance, gaming or other purposes. Through the present question the researcher has tried to find out the dependency level among students of central universities in Uttar Pradesh.

Table 6.27 shows that 99.7% (598 out of 600) respondents responded to this question while 0.3% (2 out of 600) respondents did not respond to this question.

**Table 6.27:** Case Summary of $Purpose

| | Cases Summary | | | | | |
|---|---|---|---|---|---|---|
| | Valid | | Missing | | Total | |
| | N | Percent | N | Percent | N | Percent |
| $Purpose[a] | 598 | 99.7% | 2 | 0.3% | 600 | 100.0% |

a. Dichotomy group tabulated at value 1.

Table 6.28 shows that the highest response is 498 in terms of education, which suggests that social media users use social media for education purpose at the top; this total represents 29.20% of total response given (498/1708), but 83.6% of the cases (498/598) followed by communication and entertainment purpose.

**Table 6.28:** Percentage of Cases of $Purpose

| | | Responses | | Percent of Cases |
|---|---|---|---|---|
| | | N | Percent | |
| $Purpose[a] | Communication | 456 | 26.7% | 76.5% |
| | Education | 498 | 29.2% | 83.6% |
| | Entertainment | 377 | 22.1% | 63.3% |
| | Shopping | 178 | 10.4% | 29.9% |
| | Finance | 111 | 6.5% | 18.6% |
| | Gaming | 73 | 4.3% | 12.2% |
| | Others | 15 | 0.9% | 2.5% |
| **Total** | | **1708** | **100.0%** | **286.6%** |

a. Dichotomy group tabulated at value 1.

**Q. 9. When you hear the word privacy, what comes to your mind?**

Privacy is a sweeping concept, encompassing inter alia freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations. The researcher has tried to know the privacy perceptions among students of central universities in Uttar Pradesh through question no. 9.

Table 6.29 shows that 98.8% (593 out of 600) respondents responded to this question, while as 1.2% (7 out of 600) respondents did not respond to this question.

**Table 6.29:** Case Summary of $Privacy

| | Cases | | | | | |
|---|---|---|---|---|---|---|
| | Valid | | Missing | | Total | |
| | N | Percent | N | Percent | N | Percent |
| **$Privacy[a]** | 593 | 98.8% | 7 | 1.2% | 600 | 100.0% |

a. Dichotomy group tabulated at value 1.

Table 6.30 shows the researcher received 1898 responses in total. The highest response is 429 in terms of information privacy, which suggests that whenever social media users hear the word 'privacy' majority of the users perceive 'information privacy' as a privacy; this total represents 22.6% of total response given (429/1898), but 72.3% of the cases (429/593). The table also shows that -14.8% respondents (280/1898) perceive privacy as bodily privacy, communication privacy, informational privacy, territorial privacy as whole; but 47.2% of the cases (280/593).

**Table 6.30:** Percentage of Cases of $Privacy

| | | Responses | | Percent of Cases |
|---|---|---|---|---|
| | | N | Percent | |
| $Privacy[a] | **Bodily Privacy** | 402 | 21.2% | 67.8% |
| | **Communicational Privacy** | 426 | 22.4% | 71.8% |
| | **Informational Privacy** | **429** | **22.6%** | **72.3%** |
| | **Territorial Privacy** | 323 | 17.0% | 54.5% |
| | **All of Above** | **280** | **14.8%** | **47.2%** |
| | **None of Above** | 13 | 0.7% | 2.2% |
| | **Any Others** | 25 | 1.3% | 4.2% |
| **Total** | | **1898** | **100.0%** | **320.1%** |

a. Dichotomy group tabulated at value 1.

**Q. 10. How informational privacy can be best described?**

Informational privacy is one of the integral parts of privacy discourse in the digital age. One of the most predominant theories of privacy is that of control over personal information. According to Alan Westin, "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others".[32] Researcher has tried to know the informational privacy perception among students of central universities in Uttar Pradesh.

Table 6.31 shows that 98.8% (593 out of 600) respondents responded to this question, while 1.2% (7 out of 600) respondents did not respond to this question.

**Table 6.31:** Case Summary of $Informational_Privacy

| | Cases | | | | | |
|---|---|---|---|---|---|---|
| | Valid | | Missing | | Total | |
| | N | Percent | N | Percent | N | Percent |
| $Informational_Privacy[a] | 593 | 98.8% | 7 | 1.2% | 600 | 100.0% |

a. Dichotomy group tabulated at value 1.

**Table 6.32:** Percent of Cases of $Informational_Privacy

| | | Responses | | Percent of Cases |
|---|---|---|---|---|
| | | N | Percent | |
| $Informational_Privacy[a] | **Freedom From Intrusion** | 333 | 18.2% | 56.2% |
| | **Right To Let Alone** | 365 | 20.0% | 61.6% |
| | **Human Dignity** | 324 | 17.8% | 54.6% |
| | **Email_Telephone** | 337 | 18.5% | 56.8% |
| | **ClaimTo Determine** | 261 | 14.3% | 44.0% |
| | **All_2** | 205 | 11.2% | 34.6% |
| **Total** | | 1825 | 100.0% | 307.8% |

a. Dichotomy group tabulated at value 1.

Table 6.32 shows the researcher received 1825 responses in total. 333 response support 'Freedom from intrusion'; this total represents 18.2% of total response given (333/1825), but 56.2% of the cases (333/593). 365 responses were received in favour of 'Right to be Let Alone'; this total represents 20.0% of total response given (365/1825)

[32] Alan Westin, *Privacy and Freedom* 1 (IG Publishing, New York, 1967).

but 61.6% of the cases (365/593). 324 response support 'Human Dignity' as part of informational privacy; this total represents 17.8% of total response given (324/1825) but 54.6% of the cases (324/593). 337 responses from respondents reveal that these respondents perceive informational privacy as 'protection of communication done via email and telephone'; this total represents 18.5% of total response given (337/1825) but 56.8% of the cases (337/593). 261 response support 'claim of individuals, groups, or institutions to determine to whom their personal information is shared with' as informational privacy; this total represents 14.3% of total response given (261/1825) but 44% of the cases (261/593). 205 responses convey that 'Freedom from Intrusion', 'Right to Let Alone', 'Human Dignity', 'email_telephone', 'claim_ to Determine' all are part of informational privacy; this total represents 11.2% of total response given (205/1825) but 34.6% of the cases (205/593).

Thus, the highest response is 365 (20.0%) in terms of 'Right to Let Alone' which suggests that whenever social media users hear the word 'informational privacy' majority of the users perceive it as 'Right to Let Alone' while as only 261 (14.3%) responses perceive informational privacy in consonance of Prof Alan Westin view as 'claim of individuals, groups, or institutions to determine to whom their personal information is shared with'.

**11.What kind of personal information shared by you is collected by social networking sites /apps?**

Social Media enterprises have built business models reliant on a currency of personal data. Individuals depend on free accesses to many services, from search engines to price comparison, social networking sites and media services such as YouTube, Facebook, Twitter, Google and many more. Symbiotic relations of individuals with online commercial enterprises facilitate social networking sites and apps to gather personal data of users through various overt and covert means in return of so-called free services of SNSs/Apps. Social networking sites and apps collect users account information, contact information, payment information, location information, device information. The researcher has tried to know the awareness level of targeted group social media users through this question.

Table 6.33 shows that 99.2% (595 out of 600) respondents responded to this question, while 0.8% (5 out of 600) respondents did not respond to this question.

**Table 6.33:** Case Summary of $Information_Collected

| | Cases | | | | | |
|---|---|---|---|---|---|---|
| | Valid | | Missing | | Total | |
| | N | Percent | N | Percent | N | Percent |
| $Information_Collected[a] | 595 | 99.2% | 5 | 0.8% | 600 | 100.0% |

a. Dichotomy group tabulated at value 1.

**Table 6.34:** Percentage of Cases $Information_Collected

| | | Responses | | Percent of Cases |
|---|---|---|---|---|
| | | N | Percent | |
| Personal Information Collected[a] | **Account_Information** | 445 | 25.2% | 74.8% |
| | **Contact_Info** | 357 | 20.2% | 60.0% |
| | **Payment_Info** | 213 | 12.1% | 35.8% |
| | **Location_Info** | 290 | 16.4% | 48.7% |
| | **Device_Info** | 243 | 13.8% | 40.8% |
| | **All Above** | 169 | 9.6% | 28.4% |
| | **Do Not Know** | 47 | 2.7% | 7.9% |
| **Total** | | **1764** | **100.0%** | **296.5%** |

a. Dichotomy group tabulated at value 1.

Table 6.34 shows the researcher received 1764 responses in total. 445 responses reflect that account information is collected by SNSs/Apps, this total represents 25.2% of total response given (445/1764) but 74.8% of the cases (445/595). While 357 responses show that contact information is collected by SNSs/Apps; this total represents 20.2% of total response given (357/1764) but 60% of the cases (357/595). Payment information is collected by the SNSs/Apps as opined by 213 respondents; this total represents 12.1% of total response given (213/1764) but 35.8% of the cases (213/595). 290 respondents have opined that location information is collected by SNSs/Apps; this total represents 16.4% of total response given (290/1764) but 48.7% of the cases (290/595). 243 respondents replied that device information is collected by SNS/Apps; this total represents 13.8% of total response given (243/1764) but 40.8% of the cases (243/595). Only 169 respondents have perception that all kind of information i.e., account information, contact information, payment information, location information, device information is collected by social networking sites and apps; this total represents 9.6% of total response given (169/1764) but 28.4% of the cases (169/595). While 47 respondents don't have any clue to answer this question; this total represents 2.7% of total response given (47/1764) but 7.9% of the cases (47/595).

**Q. 12. For what purpose social networking sites / apps do use your personal information?**

One of the basic purposes of collection of users information by the SNSs/Apps is to generate revenue through advertisement. Apart from advertisements, social media claims that personal data collected by them is to provide better services, develop new services and sharing users' data with law enforcement agencies on demand. The researcher has tried to know the awareness level of targeted users regarding for what purpose personal information is collected by SNSs/Apps.

Table 6.35 shows that 98.8% (593 out of 600) respondents responded to this question, while 1.2% (7 out of 600) respondents did not respond to this question.

**Table 6.35:** Case Summary of $Collection_Purpose

| | Cases | | | | | |
|---|---|---|---|---|---|---|
| | Valid | | Missing | | Total | |
| | N | Percent | N | Percent | N | Percent |
| $Collection_Purpose[a] | 593 | 98.8% | 7 | 1.2% | 600 | 100.0% |

a. Dichotomy group tabulated at value 1

Table 6.36 shows that the total received responses is 1419. 389 respondents answered that social media collects personal data of users for advertisement purposes; this total represents 27.4% of total response given (389/1419) but 65.6% of the cases (389/593). 316 respondents opined that social media collect personal data of users for providing better services; this total represents 22.3% of total response given (16/1419) but 53.3% of the cases (316/593). To provide new services, data of users is collected by social media as responded by 261 participants; this total represents 18.4% of total response given (261/1419) but 44.0% of the cases (261/593). 214 respondents say that social media collect users' data for sharing with law enforcement agencies; this total represents 15.1% of total response given (214/1419) but 36.1% of the cases (214/593). 164 respondents opined that social media collects data of users for advertisement purpose, for providing better and new services and for sharing with law agencies; this total represents 11.6% of total response given (164/1419) but 27.7% of the cases (164/593). While 75 respondents don't have any clue to answer this question; this total represents 5.3% of total response given (75/1419) but 12.6% of the cases (47/593).

**Table 6.36:** Percent of Cases of $Collection_Purpose

| | | Responses | | Percent of Cases |
|---|---|---|---|---|
| | | N | Percent | |
| $Collection_Purpose[a] | Advertisement Purpose | 389 | 27.4% | 65.6% |
| | Better_Services | 316 | 22.3% | 53.3% |
| | New_Services | 261 | 18.4% | 44.0% |
| | Share_Law_Agency | 214 | 15.1% | 36.1% |
| | All Above | 164 | 11.6% | 27.7% |
| | Can't Say | 75 | 5.3% | 12.6% |
| Total | | 1419 | 100.0% | 239.3% |

a. Dichotomy group tabulated at value 1

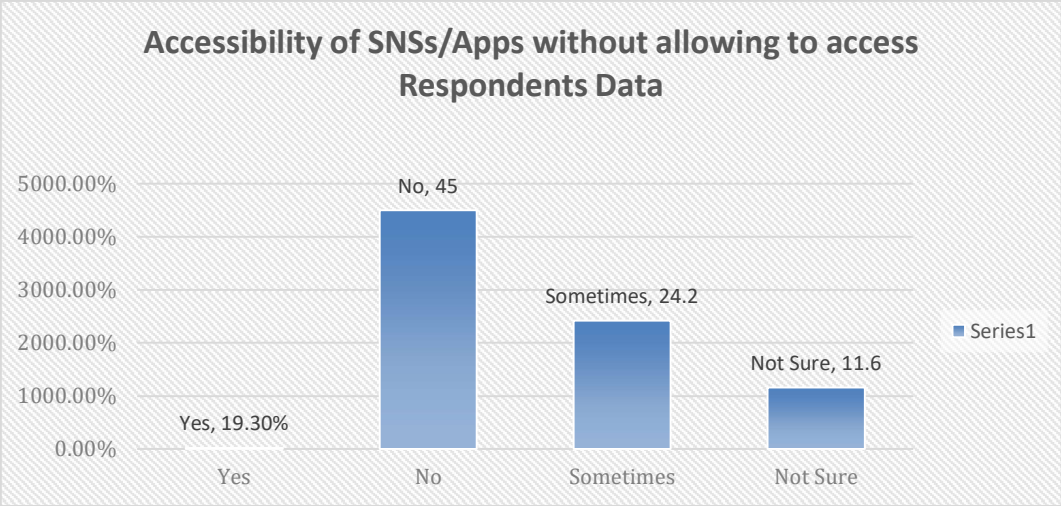
**Q.13. Can you access any social networking sites /apps without allowing to access images, videos, recording of call, files to social networking sites/app?**

Most of the social networking sites/apps are coercive in nature in the sense that users can't use their services unless they allow SNSs/Apps to access images, videos, recording of calls and other files on their devices. The researcher has tried to know the responses of targeted social media users regarding above mentioned questions. The table 6.37 and Figure 6.38 indicate that the majority 45% (268 out of 600) of the respondents replied negatively while as 19.3% (115 out of 600) replied positively. 24.2% (144 out of 600) replied that sometimes they are able to access social networking sites /apps without allowing to access images, videos, recording of call, files to social networking sites/app, 11.6% (69 out of 600) are not sure about this question while 0.7% respondents (4 out of 600) did not respond to this question.

**Table 6.37:** Frequency Table of Accessing SNS

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Yes | 115 | 19.2 | 19.3 | 19.3 |
| | No | 268 | 44.7 | 45.0 | 64.3 |
| | Sometimes | 144 | 24.0 | 24.2 | 88.4 |
| | Not Sure | 69 | 11.5 | 11.6 | 100.0 |
| | Total | 596 | 99.3 | 100.0 | |
| Missing | System | 4 | .7 | | |
| Total | | 600 | 100.0 | | |

**Figure 6.38:** Accessibility of SNSs/Apps and Respondents Data




**Q.14. Do you read all the terms and conditions of social networking sites/Apps at the time of registration?**

One of the major issues in the domain of social media is that the privacy policies are presented in such a complex fashion that it seems a long boring document with ambiguous and misleading language that is one of the reasons most users do not read them. Multiple studies in privacy policy readability found that although privacy policies are the only means for an organization to communicate data sharing and collection policies, the ambiguous, vague, and confusing language used undermines the effectiveness and purpose of the privacy policy.

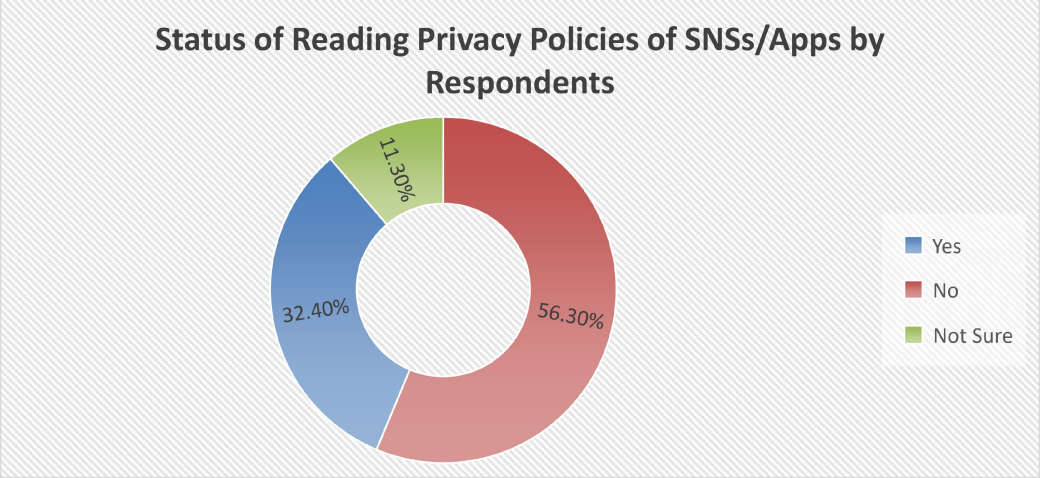
**Table 6.39:** Reading Privacy Policies Habits

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Yes | 193 | 32.2 | 32.4 | 32.4 |
| | No | 335 | 55.8 | 56.3 | 88.7 |
| | Not Sure | 67 | 11.2 | 11.3 | 100.0 |
| | Total | 595 | 99.2 | 100.0 | |
| Missing | System | 5 | .8 | | |
| Total | | 600 | 100.0 | | |

Through the above-mentioned question, the researcher has tried to know the trends among targeted social media users in the present study towards their reading terms and conditions of social networking sites and apps. Table 6.39 and Figure 6.40

show that Majority of the respondents 56.3% (335 out of 600) do not read privacy policies/ Terms and Conditions, 32.4 % (193 out of 600) respondents replied positively. 11.3 % (67 out of 600) respondents are not sure whether they read privacy policies or not while 0.8% (5 out of 600) did not respond to this question.

**Figure 6.40:** Status of reading privacy policies




**Q. 15. Do you give expressed consent to SNSs/apps to share your personal information with third parties / advertisers?**

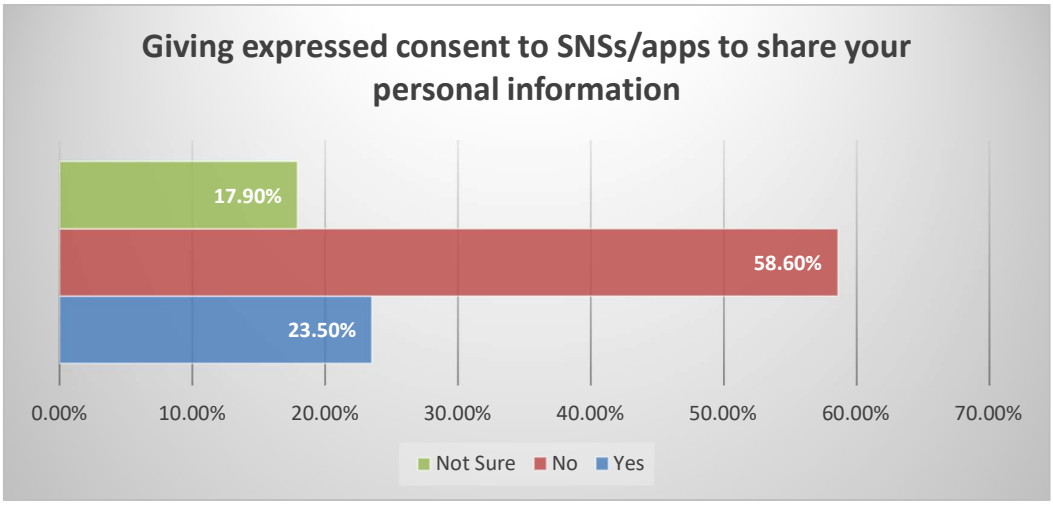
Consent is one of the complex issues in the domain of social media. It is crucial that the issue of consent is understood better by the users. On Social networking sites and apps the kind of consent generally gained is by a user scrolling down a long page of writing that they do not read and then clicking 'OK' at the end to confirm that they have 'read and understood' the terms and conditions. The information thus presented (but rarely read) is deemed 'to make the consent informed', while the clicking of OK is deemed to make it 'express'.

**Table 6.41:** Expressed consent to share users' data

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| **Valid** | **Yes** | 139 | 23.2 | 23.5 | 23.5 |
| | **No** | 347 | 57.8 | 58.6 | 82.1 |
| | **Not Sure** | 106 | 17.7 | 17.9 | 100.0 |
| | **Total** | 592 | 98.7 | 100.0 | |
| **Missing** | **System** | 8 | 1.3 | | |
| **Total** | | **600** | **100.0** | | |

Table 6.42 and Figure 7.40 show that the majority of the respondents 58.6% (347 out of 600) do not give expressed consent to SNSs/Apps to share their personal information with third parties/advertisers; while as 23.5% (139 out of 600) give expressed consent. 17.9% (106 out of 600) respondents are not sure whether they give expressed consent or not to the SNSs/Apps to share their personal data to third parties while as 1.3% (8 out of 600) respondents did not respond to this question.

**Figure: 6.42** Giving Consent to share personal information



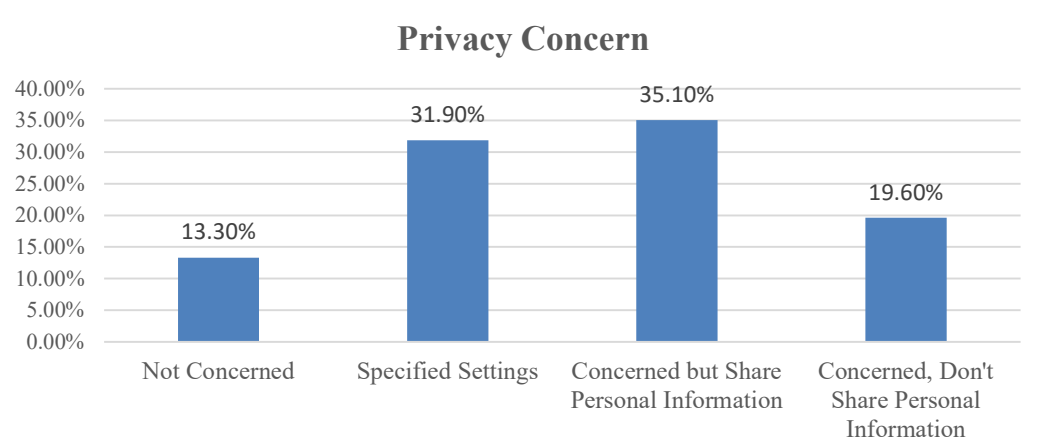

**Q.16. How do you concern about privacy of your personal information on social media?**

**Table 6.43:** Privacy Concern of Personal Information

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Not Concerned | 79 | 13.2 | 13.3 | 13.3 |
| | Specified Settings | 189 | 31.5 | 31.9 | 45.3 |
| | Concerned but Share Personal Information | 208 | 34.7 | 35.1 | 80.4 |
| | Concerned, Don't Share Personal Information | 116 | 19.3 | 19.6 | 100.0 |
| | Total | 592 | 98.7 | 100.0 | |
| Missing | System | 8 | 1.3 | | |
| Total | | 600 | 100.0 | | |

Through this question the researcher has made efforts to know that in what manners respondents concern about privacy over social media platforms. Table 6.43 and Figure 6.44 show that 13.3% (79 out of 600) respondents do not concern about privacy of personal information on social media, while as 31.9% (189 out of 600) respondents specified settings, 35.1% (208 out of 600) respondents are concerned about personal information but still share personal information, 19.6% (116 out of 600) respondents shown their concern; they don't share their personal information. 1.3% (8 out 600) did not respond to this question.

**Figure 6.44:** Privacy Concern of Personal Data



**Q.17. How do you limit social networking sites / apps to collect your personal information?**

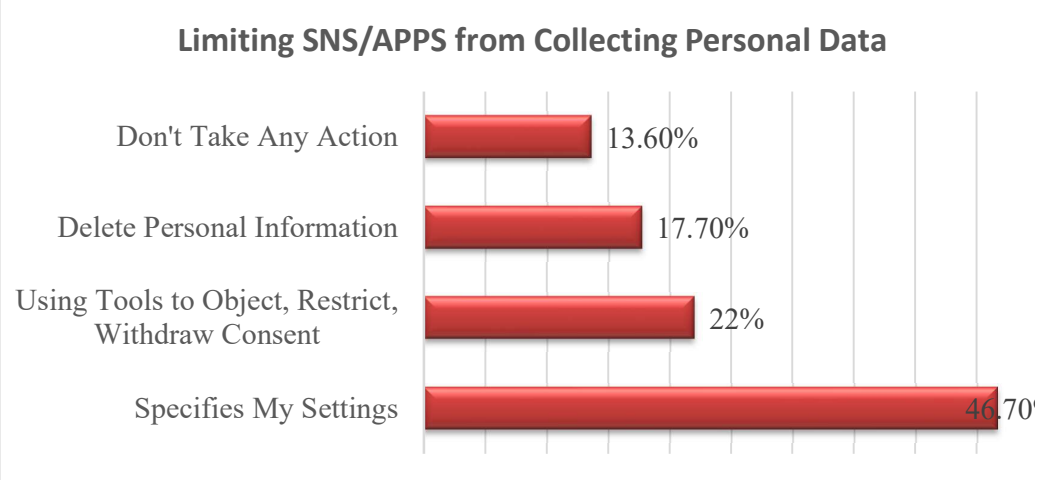
Social Networking sites and Apps in consonance with universally accepted data protection principles, rights of data subjects, and corporate social responsibility provide a certain mechanism in order to limit social networking sites and apps to collect users' personal information. Specify Settings, using tools to object, restrict, withdraw consent, delete personal information are certain options available on sites to limit SNSs/Apps to collect personal information.

The researcher through the present question has tried to know the trends how respondents limit social networking sites and apps to collect personal information of respondents. Table 6.45 and Figure 6.46 show that 46.7% (274 out of 600) respondents specify settings, 22% (129 out of 600) respondents use tools to object, restrict, withdraw consent, 17.7% (104 out of 600) respondents delete personal information, while as 13.6% (80 out of 600) respondents don't take any action. 2.2% (13 out of 600) did not respond to this question.

**Table 6.45:** Limiting SNSs/Apps from collecting Personal Information

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Specifies My Settings | 274 | 45.7 | 46.7 | 46.7 |
| | Using Tools to Object, Restrict, Withdraw Consent | 129 | 21.5 | 22.0 | 68.7 |
| | Delete Personal Information | 104 | 17.3 | 17.7 | 86.4 |
| | Don't Take Any Action | 80 | 13.3 | 13.6 | 100.0 |
| | Total | 587 | 97.8 | 100.0 | |
| Missing | System | 13 | 2.2 | | |
| Total | | 600 | 100.0 | | |

**Figure 6.46:** Limiting SNSs/Apps



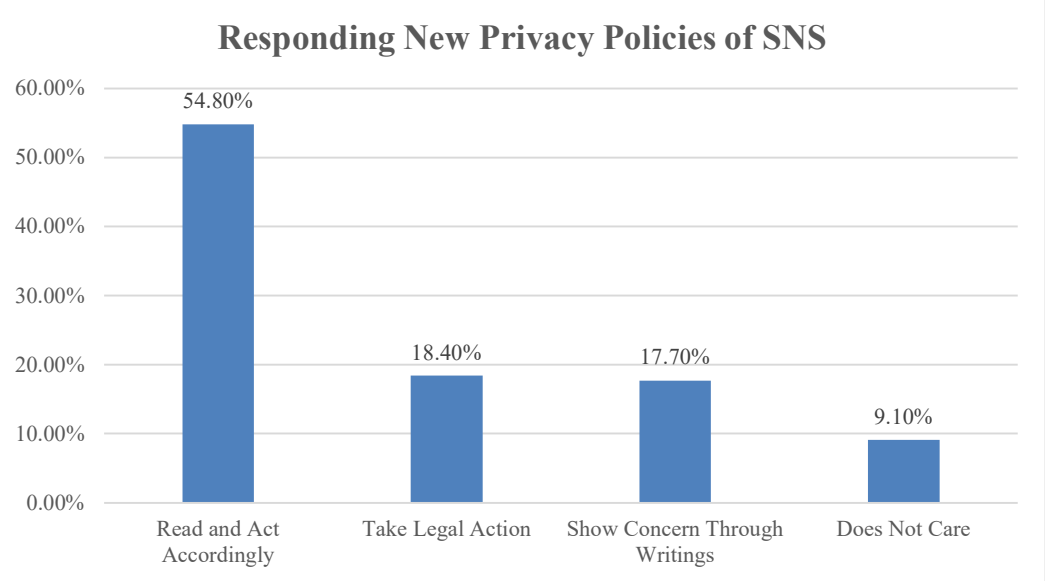

**Q. 18. How do you respond when new privacy policies of social networking sites /apps are notified and informed you at your mobile?**

**Table 6.47:** Responding New Policy

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Read and Act Accordingly | 313 | 52.2 | 54.8 | 54.8 |
| | Take Legal Action | 105 | 17.5 | 18.4 | 73.2 |
| | Show Concern Through Writings | 101 | 16.8 | 17.7 | 90.9 |
| | Does Not Care | 52 | 8.7 | 9.1 | 100.0 |
| | Total | 571 | 95.2 | 100.0 | |
| Missing | System | 29 | 4.8 | | |
| Total | | 600 | 100.0 | | |

Table 6.47 and Figure 6.48 show that only 54.8% respondents read new privacy policies of SNSs and act accordingly; while as 18.5% respondents opined that they take legal action against discriminatory privacy polices of SNSs while as 17.7% respondents show their concern toward privacy polices of SNSs/Apps through writings; while as 9.1% respondents say that they don't care ambiguous, coercive, deceptive privacy policies of social networking sites and apps; while as 4.8% respondents did not respond to this question.

**Figure 6.48:** Responding New Privacy Policies




**19. What are the rights of Data Subjects (Social Media Users)?**

Some of the state legislations in the world, for example in U.K., latest EU GDPR, have provisions of rights for data subjects. As per the law SNSs/Apps must inform data subjects about the manner in which processing of the information is done. Some of the rights of data subjects are 'right of access'; 'right to be informed of the logic in automatic decision taking'; 'right to compensation'; 'right to rectify inaccurate data'; 'right to complain to ICO'; 'right to go to court' etc. The researcher has made efforts to know the awareness among respondents about their rights on social media platforms.

Table 6.49 shows that 97.8% (587 out of 600) respondents responded to this question, while 2.2% (13 out of 600) respondents did not respond to this question.

**Table 6.49:** Case Summary of $Rights_Data_Subject

| | Cases | | | | | |
|---|---|---|---|---|---|---|
| | Valid | | Missing | | Total | |
| | N | Percent | N | Percent | N | Percent |
| **$Rights_Data_Subject[a]** | 587 | 97.8% | 13 | 2.2% | 600 | 100.0% |

a. Dichotomy group tabulated at value 1.

Table 6.50 shows that the total received responses is 1641. 389 respondents answered that 'Right to Information' is data subject right; this total represents 23.8% of total response given (390/1641) but 66.4% of the cases (390/587). 'Right to Access' is a data subject right, answered by 339 respondents; this total represents 20.7% of total response given (339/1641) but 57.8% of the cases (339/587). 295 respondents view 'Right to withdraw consent' as a data subject right; this total represents 18% of total response given (295/1641) but 50.3% of the cases (295/587). 'Right to delete data' as a data subject right is answered by 290 respondents; this total represents 17.7% of total response given (290/1641) but 49.4% of the cases (290/587). Only 226 respondents perceive all the above-mentioned rights as data subject rights; this total represents 13.8% of total response given (226/1641) but 38.5% of the cases (290/587). 11 respondents opine that none of the above is data subject right; this total represents 0.7% of total response given (11/1641) but 1.9% of the cases (11/587). 90 respondents don't have a clue to this question; this total represents 5.5% of total response given (90/1641) but 15.3% of the cases (90/587).

**Table 6.50:** Percent of Cases of $Rights_Data_Subject

| | | Responses | | Percent of Cases |
|---|---|---|---|---|
| | | N | Percent | |
| $Rights_Data_Subject[a] | Right To Information | 390 | 23.8% | 66.4% |
| | Right To Access | 339 | 20.7% | 57.8% |
| | Right To Withdraw Consent | 295 | 18.0% | 50.3% |
| | Right To Delete Data | 290 | 17.7% | 49.4% |
| | All Above | 226 | 13.8% | 38.5% |
| | None of the Above | 11 | 0.7% | 1.9% |
| | Not Sure | 90 | 5.5% | 15.3% |
| Total | | 1641 | 100.0% | 279.6% |

a. Dichotomy group tabulated at value 1.

**Q.20. Right to Privacy is**

Right to Privacy has occupied a prominent place in international law. Privacy has enshrined as a right under 12 of Universal Declaration of Human Right, International Covenant on Civil and Political Rights, 1966 contains a nearly identical formulation under article 17. Apart from UDHR and ICCPR, privacy is protected in many regional instruments. Many states in the world have borrowed privacy's provision from article 12 of UDHR and incorporated it in their constitution. The Hon'ble Supreme Court of India in Puttaswamy[33] Case recognised right to privacy as a fundamental right under article 21 of the constitution and further held that privacy is a natural right that inheres in all natural persons, and that the right may be restricted only by state action that passes each of the three tests based on legality, necessity and proportionality.

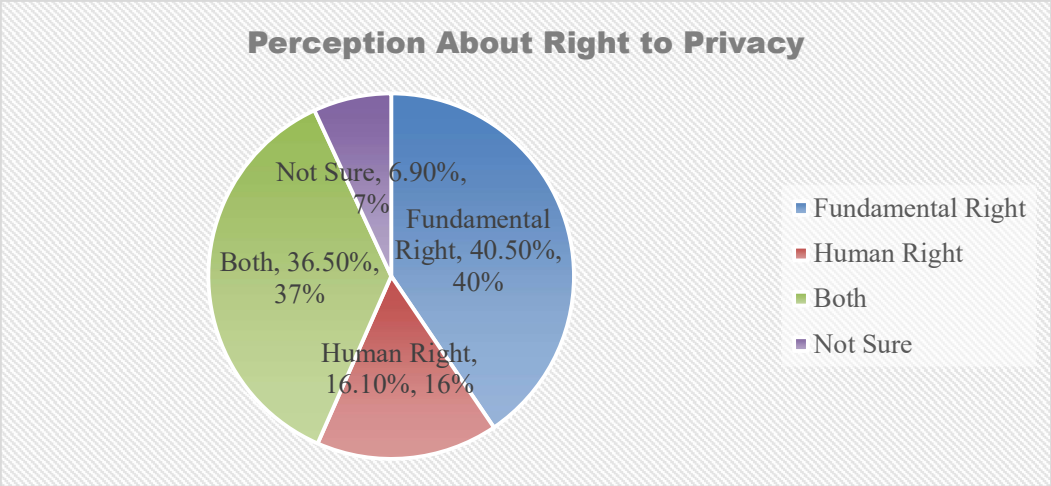
The researcher has tried to know the legal awareness among the respondents about the right to privacy through the present question. Table 6.51 and Figure 6.52 show that 40.5% (241 out of 600) respondents have perception that right to privacy is a fundamental right, 16.1% (96 out of 600) believe that privacy is a basic human right, 36.5% (217 out of 600) respondents opined that privacy is a fundamental right as well as basic human right both, 6.9% (41 out of 600) respondents don't have any clue to answer to this question while as 0.8% (5 out of 600) respondents did not respond to this question.

**Table 6.51:** Right to Privacy Awareness

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | **Fundamental Right** | 241 | 40.2 | 40.5 | 40.5 |
| | **Human Right** | 96 | 16.0 | 16.1 | 56.6 |
| | **Both** | 217 | 36.2 | 36.5 | 93.1 |
| | **Not Sure** | 41 | 6.8 | 6.9 | 100.0 |
| | **Total** | 595 | 99.2 | 100.0 | |
| **Missing** | **System** | 5 | .8 | | |
| **Total** | | 600 | 100.0 | | |

[33] (2017) 10 SCC 1

**Figure 6.52:** Perception about right to privacy




**Q.21. Is Imposition and implementation of policy (like installation of Arogyasetu in your mobile) without proper legislation a violation of Human Right?**

In the wake of COVID-19, use of information and communication technology and surveillance by the State has met at cross-roads and has given much leeway for the State to cause mass-surveillance.[34] It was alleged that the government's technology solutions (Arogya Setu App) to fight COVID-19 do not meet minimum legal requirements (legality, necessity and proportionality as per the judgement of Puttaswamy Case).[35] Hence' state violates right to privacy of COVID-19 affected persons.

**Table: 6.53:** Arogyasetu and Violation of Human Rigths

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| **Valid** | **Yes** | 282 | 47.0 | 47.3 | 47.3 |
| | **No** | 199 | 33.2 | 33.4 | 80.7 |
| | **Not Sure** | 115 | 19.2 | 19.3 | 100.0 |
| | **Total** | 596 | 99.3 | 100.0 | |
| **Missing** | **System** | 4 | .7 | | |
| **Total** | | 600 | 100.0 | | |

[34] Yuthika Bhargava, "Hacker sees security flaws in Arogya Setu" *Th Hindu,* May 06, 2020.
[35] Suhrith Parthasarathy, Gautam Bhatia and Apar Gupta, "Privacy concerns during a pandemic" *The Hindu,* April 29, 2020.

**Figure: 6.54** Arogyasetu and Human Rights

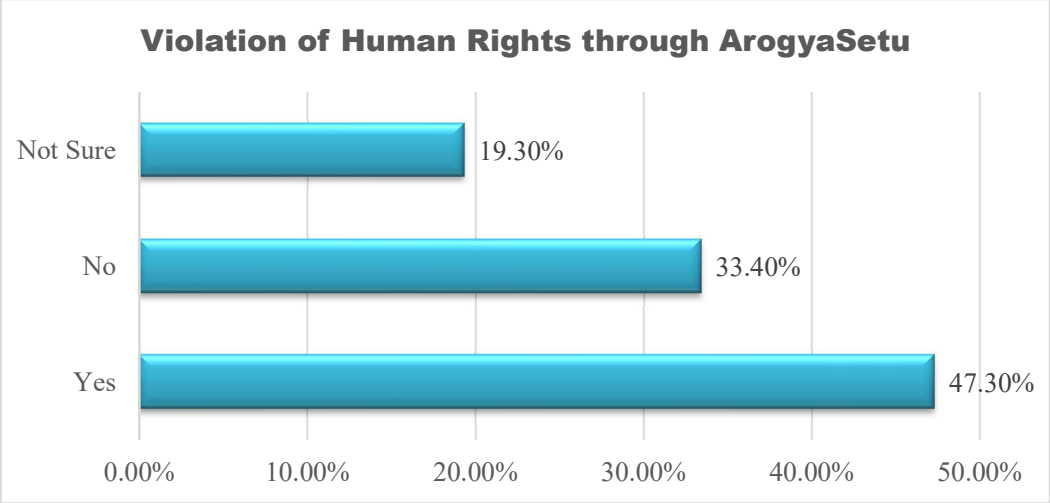



Table 6.53 and Figure 6.54 show that 47.3% (282 out of 600) respondents opined that Imposition and implementation of policy (like installation of Arogyasetu in your mobile) without proper legislation is a violation of Human Right; while as 33.4% (199 out of 600) respondents believe that it's not a violation of human right if state asks its citizen to install Arogyasetu App in their mobile; 19.3% (115 out of 600) not sure about the answer of the question; while as .7% ( 4 out of 600) respondents did not respond to this question.

**Q.22. Does Government of India have proper legislation to deal with protection of privacy of citizens in online social media?**

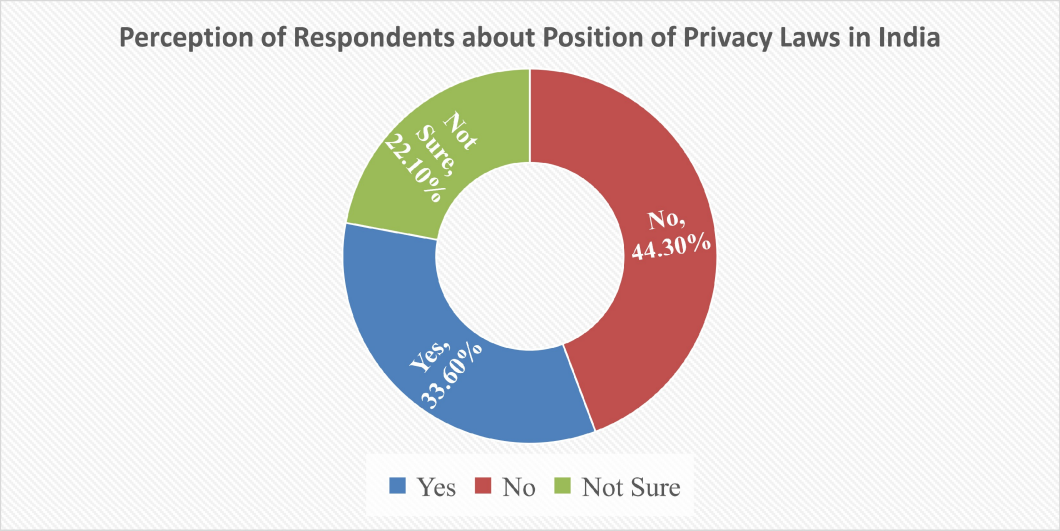
India does not have any specific law for data protection. Statutory protection of privacy can be found in India is scattered across a number of statutes. For information and technology related disputes, citizens of the country have to rely on the provisions of The Information Technology Act 2000 (IT Act), as amended by the Information Technology (Amendment) Act 2008 (ITAA). In February, 2021 the Ministry of Electronics and Information Technology, Government of India has notified new rules under the Information Technology Act, 2000 known as 'Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, for monitoring social media digital media platform. The personal data protection bill 2019 is still pending. The researcher has made efforts to know the appropriateness of the law to deal with protection of privacy of citizens in online social media.

Table 6.55 and Figure 6.56 show that 33.6% (201 out of 600) respondents have perception that Government of India have proper data protection law, while as majority of the respondents 44.3% (265 out of 600) replied negatively, 22.1% (132 out of 600) respondents are not sure about answer to this question while as 0.3 (2 out of 600) did not respond to this question.

**Table 6.55:** Perception about privacy laws in India

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| **Valid** | **Yes** | 201 | 33.5 | 33.6 | 33.6 |
| | **No** | 265 | 44.2 | 44.3 | 77.9 |
| | **Not Sure** | 132 | 22.0 | 22.1 | 100.0 |
| | **Total** | 598 | 99.7 | 100.0 | |
| **Missing** | **System** | 2 | .3 | | |
| **Total** | | 600 | 100.0 | | |

**Figure 6.56:** Privacy Laws in India




**23. What do you expect from social networking sites and apps while processing of your personal data?**

It is obligatory for the social networking sites and apps to adhere to the universally accepted data protection principles like Collection Limitation Principle, Data Quality Principle, Purpose Specification Principle, Use Limitation Principle, Security

Safeguards Principle, Openness Principle, Individual Participation Principle, and Accountability Principle while processing personal data of data subjects. Through the present question the researcher has made efforts to know the legal awareness of respondents regarding data protection principles.

Table 6.57 shows that 98.8% (593 out of 600) respondents responded to this question, while 1.2% (7 out of 600) respondents did not respond to this question.

**Table 6.57:** Case Summary of $Data_Protection_Principles

| | Cases | | | | | |
|---|---|---|---|---|---|---|
| | Valid | | Missing | | Total | |
| | N | Percent | N | Percent | N | Percent |
| $Data_Protection_Principles[a] | 593 | 98.8% | 7 | 1.2% | 600 | 100.0% |

**a.** Dichotomy group tabulated at value 1

**Table 6.58:** Percent of Cases of $Data_Protection_Principles

| | | Responses | | Percent of Cases |
|---|---|---|---|---|
| | | N | Percent | |
| $Data_Protection_Principles[a] | Fair & Lawful | 374 | 24.9% | 63.1% |
| | Purpose Limitation | 317 | 21.1% | 53.5% |
| | Data Quality | 295 | 19.7% | 49.7% |
| | Data Security | 297 | 19.8% | 50.1% |
| | All Above | 201 | 13.4% | 33.9% |
| | None of Above | 17 | 1.1% | 2.9% |
| **Total** | | **1501** | **100.0%** | **253.1%** |

a. Dichotomy group tabulated at value 1.

Table 6.58 shows that total response received is 1501. 374 respondents expect that processing of personal data must be fair and lawful, this total represents 24.9% of total response (374/1501) but 63.1% of the cases (374/593); 317 respondents opined that personal data must be processed for limited purposes, this is 21.1% of total response (317/1501) but 53.5% is of the cases (317/593). 295 respondents say about data quality i.e. data must be adequate, relevant and not excessive which represents 19.7% of total response give (295/1501) but 49.7% of the cases (295/593). 297 respondents talk about data security (personal data must be secure) which is 19.8% of the total response given (297/1501) but 50.1% of cases (297/593). 201 respondents have expressed their view that while processing of personal data all data protection principles

(fair & lawful, purpose limitation, data quality, data security) must be kept in mind by the SNSs/Apps which represents 13.4% of total response given (201/1501) but 33.9% (201/593). 17 respondents replied that they do not expect any of the data protection principles to be followed by the SNSs/Apps while processing of personal data which represents 1.1% of total response given (17/1501) but 2.9% of the cases (17/593).

**Q.24. If your privacy is violated over social media platform, what action will you take for its protection?**

Although social media adopts a self-regulatory approach to run their business, but still some limited remedies are available in law. The researcher has made efforts to know what kind of actions will be taken by the respondents in case of violation of privacy over social media platforms. Table 6.59 and Figure 6.60 show that 18.7% (110 out of 600) respondents say that they will file injunction suit in court; 27.8% (164 out of 600) say that they will file complaint in either national human right commission or state human right commission; 23.3% (137 out of 600) respondents say that they will file complaint before competent authority; 27% (159 out of 600) say that they will register FIR; 3.2% (19 out of 600) respondents say that they will will take any action; 1.8% (11 out of 600) respondents did not respond to this question.

**Table 6.59:** Remedies available in case of violation of privacy

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | File Injunction Suit in Court | 110 | 18.3 | 18.7 | 18.7 |
| | File Complaint in NHRC/SHRC | 164 | 27.3 | 27.8 | 46.5 |
| | File Complaint Before Authority | 137 | 22.8 | 23.3 | 69.8 |
| | Register FIR | 159 | 26.5 | 27.0 | 96.8 |
| | Not take any action | 19 | 3.2 | 3.2 | 100.0 |
| | Total | 589 | 98.2 | 100.0 | |
| Missing | System | 11 | 1.8 | | |
| Total | | 600 | 100.0 | | |

**Figure 6.60:** Remedies in case of violation of privacy

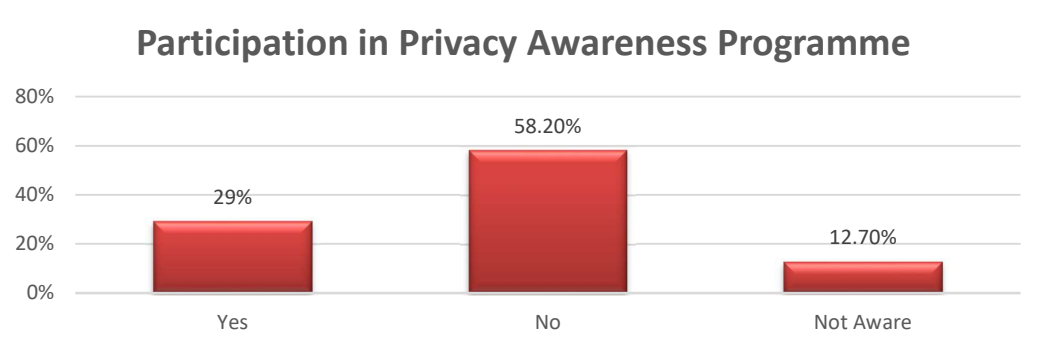

**Q.25. Have you ever participated in any program organized by your university to spread awareness about privacy/cyber issues in online social media platform?**

Table 6.61 and Figure 6.62 show that 29% (171 out of 600) respondents participated in a privacy/cyber issues awareness programme organized by the concerned university. 58.2% (343 out of 600) respondents did not participate in any privacy/cyber issues awareness programmes, 12.7% (75 out of 600) respondents are not aware about such programmes while as 1.8% (11 out of 600) did not respond to this question.

**Table 6.61:** Participation in Awareness Program

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Yes | 171 | 28.5 | 29.0 | 29.0 |
| | No | 343 | 57.2 | 58.2 | 87.3 |
| | Not Aware | 75 | 12.5 | 12.7 | 100.0 |
| | Total | 589 | 98.2 | 100.0 | |
| Missing | System | 11 | 1.8 | | |
| Total | | 600 | 100.0 | | |

**Figure: 6.62:** Privacy Awareness Programme



## 6.6 PART B: DATA SHOWING PRIVACY CONCERNS OF CENTRAL UNIVERSITIES IN UTTAR PRADESH

Part B is based on information received from central universities in response to seven queries of the researcher asked in the form of Right to Information 2005 application. Information received from central universities in Uttar Pradesh has been analysed as below:

**Table: 6.63** Status of Information received from central universities in Uttar Pradesh

| Name of University | Whether Information received from central universities or not (Yes/No) |
|---|---|
| Aligarh Muslim University, Aligarh | Yes |
| Babasaheb Bhimrao Ambedkar University, Lucknow | No |
| Banaras Hindu University, Varanasi | Yes |
| Rani Lakshmi Bai Central Agricultural University, Jhansi | No |
| Rajiv Gandhi National Aviation University, Amethi | No |
| University of Allahabad, Prayagraj | No |

Table 7.61 shows the status of Information Received from Central Universities in Uttar Pradesh in response to research scholar's queries regarding privacy concerns. Table 7.61 shows that only two universities Aligarh Muslim University (Aligarh) and Banaras Hindu University (Varanasi) responded to queries of the researcher while as other universities Babasaheb Bhimrao Ambedkar University (Lucknow), Rani Lakshmi Bai Central Agricultural University (Jhansi), Rajiv Gandhi National Aviation University (Amethi), University of Allahabad (Prayagraj) did not respond to the queries of the researcher.

From Figure 6.64 it is clear that only 33.33% universities responded to the queries of the researcher while 66.67% universities did not respond to the queries.

**Figure 6.64:** RTI response from universities

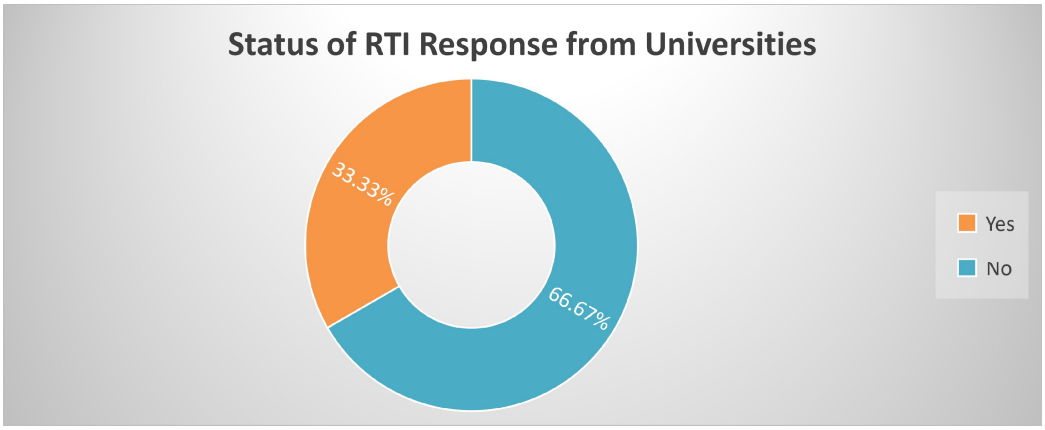


**Table 6.65:** Information received through RTI from Central Universities in U.P.

| Queries raised in RTI application | Response received from Aligarh Muslim University (Aligarh) | Responses from Banaras Hindu University (Varanasi) |
|---|---|---|
| What kind of social networking sites and apps university is using for imparting online education or intercommunication with staffs? a. GoogleMeet b. Zoomc. Webexd. Facebook e. YouTube<br>f. Others …… | 1. Multiple platforms including Google Meet, Zoom, YouTube, Moodle LMS etc. are being used various Faculties, Departments, OUs as per the number of concurrent users in the class/session/online events and preference of the individual Faculties / Departments / Colleges / Institutes. | 1.<br>) Google Meet<br>c) Webex |
| Does university have its own software/apps used for online teaching & other purpose free from violation of privacy? (a) Yes (b) No | 2. In addition to multiple secure online platforms mentioned at point number 1, University also has an on-premise institutional LMS (https://lms.amu.ac.in) which is made available at all faculty of studies for progressive adoption by all concern. | 2. No |
| Is there any policy adopted by the University to protect personal information of students, research scholars, teaching staffs and non-teaching staff? (a) Yes (b) No | 3. University has adopted IT Policy and guidelines, a copy of the same is available at public domain (https://api.amu.ac.in/storage/file/pdf/cc/ITP.pdf) | 3. Privacy Policy as available on BHU website: new.bhu.ac.in |
| What measures is being taken between university and agencies (acting on behalf of university like National Testing agency and others) regarding the processing of personal information of concerned persons (students, teaching staffs, non-teaching staff) to respect, protect the right to privacy?<br>(a) Have a MOU between University and agencies not to share personal data with others.<br>(b) Delete data after reasonable time period, once purpose is fulfilled.<br>(c) Seek consent of concerned persons regarding processing of data like uploading on website | 4. Item related to another office *Admissions and Examinations,* the matter may be referred to this office. | 4. Information not available in the Computer Centre |
| Does your university's website follow any privacy policies? a. Yes b. No | 5. University has multiple websites maintained by respective computer cells like Computer Cell admissions and Examinations, Computer Cell Registrar's Office etc. Each of which is governed by IT Policy mentioned at point number | 5 a) Yes |

| | | |
|---|---|---|
| | 3. URL (www.amu.ac) is not correct however University is committed to respecting and following privacy. | |
| 6 (a) Has any department of university organized privacy awareness program for students in context of social media?<br>(b) If yes, how many such programs have been organized from January 2019 to January December 2021? | 6. Information seeker may like to pursue the university website where information may be available at multiple sections including departmental webpages (https://amu.ac.in/department-list), past events (https://amu.ac.in/events) and News Section (https://amu.ac.in/news) etc. in its quest for information. | 6. Information not available in Computer Centre |

Table 6.65 shows the Information received through RTI from two central Universities (Aligarh Muslim University and Banaras Hindu Univerity) in U.P.

In response to query no. 1 "What kind of social networking sites and apps university is using for imparting online education or intercommunication with staffs? a. Google Meet b. Zoom c. Webex d. Facebook e. YouTube f. Others" Aligarh Muslim University has replied that multiple platforms including Google Meet, Zoom, YouTube, Moodle LMS etc. are being used various Faculties, Departments, OUs as per the number of concurrent users in the class/session/online events and preference of the individual Faculties / Departments / Colleges / Institutes while as Google Meet and Webex are being used by Banaras Hindu University.

In response to query no. 2 "Does university have its own software/apps used for online teaching & other purposes free from violation of privacy? (a) Yes (b) No" Aligarh Muslim University replied that in addition to multiple secure online platforms mentioned at point number 1, University also has an on-premise institutional LMS (https://lms.amu.ac.in) which is made available at all faculty of studies for progressive adoption by all concern while as per the reply of Banaras Hindu University, it does not have its own software/apps used for online teaching & other purpose free from violation of privacy.

In response to query no. 3 "Is there any policy adopted by the University to protect personal information of students, research scholars, teaching staffs and non-teaching staff? (a) Yes (b) No" Aligarh Muslim University replied that University has adopted IT Policy and guidelines, a copy of the same is available at public domain

(https://api.amu.ac.in/storage/file/pdf/cc/ITP.pdf) while as Banaras Hindu University replied that Privacy Policy is available on BHU website: new.bhu.ac.in.

In response to query no. 4 "What measures are being taken between universities and agencies (acting on behalf of university like the National Testing Agency and others) regarding the processing of personal information of concerned persons (students, teaching staff, non-teaching staff) to respect, protect the right to privacy? (a) Have a MOU between University and agencies not to share personal data with others. (b) Delete data after a reasonable time period, once the purpose is fulfilled. (c) Seek consent of concerned persons regarding processing of data like uploading on website, Aligarh Muslim University has replied that Item related to another office *Admissions and Examinations,* the matter may be referred to this office while as Banaras Hindu University that Information not available in the Computer Centre.

In response to query no. 5 "Does your university's website follow any privacy policies? a. Yes b. No" Aligarh Muslim University has replied that University has multiple websites maintained by respective computer cells like Computer Cell admissions and Examinations, Computer Cell Registrar's Office etc. Each of which is governed by IT Policy mentioned at point number 3. URL (www.amu.ac) is not correct however University is committed to respecting and following privacy while as in response to query no. 5 Banaras Hindu University has replied positively.

In response to query no. 6 "(a) Has any department of university organized a privacy awareness program for students in the context of social media? (b) If yes, how many such programs have been organized from January 2019 to January December 2021?" Aligarh Muslim University has replied that Information seeker may like to pursue the university website where information may be available at multiple sections including departmental webpages (https://amu.ac.in/department-list), past events (https://amu.ac.in/events) and News Section (https://amu.ac.in/news) etc. in its quest for information while as Banaras Hindu University has replied that Information not available in Computer Centre.

## 6.7 FINDINGS

- Data analysis from Table 6.13 and Figure 6.14 reveals that maximum participation in the survey is from age group 18-22 i.e 34.5 % while as minimum participation is from age group of above 30 i.e. 16.3%. It reflects that those respondents of the youngest age are more addicted to social networking sites and apps.
- The male's participation in the survey is 65% (390 out of 600 sample) while as the female's participation is 35% (210 out of 600). It reflects that male are dominating in social media's activities in comparison to females.
- The maximum participation course wise is from the students pursuing post-graduation i.e. 40.3%; while minimum participation is from the students pursuing other courses including diploma i.e 10.7 %.
- Data shows that WhatsApp (16.8%) is the first choice of respondents followed by YouTube (15.0%) is the second choice while Facebook (14.1%) and Google (14.1%) are the third choice of respondents.
- Data (Table 6.23 and Figure 6.24) show that universities are partially allowing respondents to use social networking sites /apps in their cyber libraries
- Data (Table 6.26) shows that majority of the respondents i.e. 34.0% respondents prefer to communicate with others in form of text messages, while as 30.2% use images to communicate their views and expressions, 17.9% respondents post videos, 12.9% post links while as 5.1% respondents communicate in other forms.
- Data shows that (Table 6.28) majority of the respondents use social networking sites/apps for education purpose, followed by communication, others use for entertainment, shopping, finance activities, gaming purpose.
- Data (Table 6.30) show that 14.8% respondents perceive bodily privacy, communication privacy, informational privacy, territorial privacy as whole. 0.7% respondents replied that none of the options is a part of privacy. It reflects that respondents are not much aware about privacy concepts.
- Data (Table 6.32) shows that Only 14.3% respondents perceive informational privacy in consonance with Prof. Alan Westin view on informational privacy. Hence, awareness about informational privacy in the era of social media among social media users is not satisfactory.

- Social Media sites and apps are collecting users' information through overt and covert means. The researcher found in a survey (Table 6.34) that the awareness level of respondents about different types of information collected by SNSs/Apps is very low. Only 9.6% respondents have the perception that all kinds of information i.e., account information, contact information, payment information, location information, device information is collected by social networking sites and apps.
- Table 6.36 indicates that only 11.6% respondents have the perception that SNSs/Apps collect personal information of users for advertisement purposes, to provide better services, to develop new services, to share with law agencies on demand. Hence the awareness level of respondents about the purpose for which personal data of respondents is collected by SNSs/Apps is not satisfactory.
- The table 6.37 and Figure 6.38 indicate that respondents have huge diverse opinions about accessibility of SNSs/Apps without allowing access respondents' data.
- Through a survey the researcher found that (Table 6.39 and Figure 6.40) that majority of the respondents 55.8% do not read privacy policies/ Terms and Conditions of social networking sites / apps. This is alarming situation among respondents that they are not showing concerns towards privacy.
- Data shows that the majority of the respondents (57.8%) do not give expressed consent SNSs/Apps to share personal information of users to third parties while 23.5% responded positively. This reflects that SNSs/Apps receive the consent of users through coercive and deceptive manners.
- Survey (Table 6.43 and Figure 6.44) shows that 13.2% respondents do not concern about privacy of personal information on social media, 31.5% respondents specify settings, 34.7% respondents are concerned about personal information but still share personal information, 19.3% respondents shown their concern, hence they don't share their personal information. Hence, it has been found that the level of privacy concern among respondents is not satisfactory.
- Table 6.45 and Figure 6.46 show that 45.7% respondents specify settings, 21.5% respondents use tools to object, restrict, withdraw consent, 17.3% respondents delete personal information, while as 13.3% respondents don't take any action.

- The researcher found (Table 6.50) that only 13.8% respondents are aware about data subjects rights while the remaining respondents are partially aware about data subjects rights. Hence, awareness about data subject rights among respondents is not satisfactory.
- Table 6.51 and Figure 6.52 show that 40.5% (241 out of 600) respondents have perception that right to privacy is a fundamental right, 16.1% (96 out of 600) believe that privacy is a basic human right, 36.5% (217 out of 600) respondents opined that privacy is a fundamental right as well as basic human right both, 6.9% (41 out of 600) respondents don't have any clue to answer to this question while 0.8% (5 out of 600) did not respond to this question.
- Table 6.53 and Figure 6.54 show that 47.3% respondents opined that imposition and implementation of policy (like installation of Arogya setu in mobile) without proper legislation is a violation of human rights while 33.4% respondents don't think so.
- Survey (Table 6.55 and Figure 6.56) shows that 33.6% respondents have perception that the Government of India has proper data protection law, while the majority of the respondents 44.3% replied negatively.
- Table 6.58 shows that only 13.4% respondents have expressed their view that while processing personal data all data protection principles (fair & lawful, purpose limitation, data quality, data security) must be kept in mind by the SNSs/Apps. Hence, it shows that awareness about data protection principles among respondents is not satisfactory.
- The researcher found that (as Table 6.61 and Figure 6.62 reveal) majority of the respondents (57.2%) did not participate in any privacy/cyber issues awareness programmes, only 28.5% respondents participated in a privacy/cyber issues awareness programme organized by concerned university while as 12.5% respondents are not aware about such programmes.
- The researcher found that privacy concerns of central universities in Uttar Pradesh are not satisfactory. Out of six universities only Aligarh Muslim University, Aligarh and Banaras Hindu University, Varanasi responded to the queries of the researcher.
- The researcher found that university is mostly dependent on social networking sites / apps for imparting education. They don't have their own software.

- The non-responsive nature of universities depicts that no university (considered in research work) is taking any measures to protect the personal data of students, teaching staffs and non-teaching staffs to protect, respect the right to privacy of concerned persons.
- The survey shows that programmes organized by universities to make students aware about privacy/cyber related issues is negligible.

**One of the hypotheses of the present study was "awareness regarding legal provisions and privacy policies of social media among the students of central universities in Uttar Pradesh is not adequate".**

**The researcher on the basis of above findings reached the conclusion that "awareness regarding legal provisions and privacy policies of social media among the students of central universities in Uttar Pradesh is not adequate". Hence, the hypothesis is proved.**

# CHAPTER-VII

# CONCLUSION AND SUGGESTIONS

# CHAPTER VII

# CONCLUSION AND SUGGESTIONS

Privacy is an issue of profound importance around the world. Privacy is an important component of human personality.

Privacy is rapidly becoming inextricably linked to the world of digital communications and social media. Social media and social networking sites (SNS) have risen sharply in popularity and widespread use, allowing new forms of socialization, sharing, and communication between people. This new state of communication raises new privacy questions.

Online self-disclosure of personal information by social media users lies at the heart of the problem posed by social media. We are now beginning to realise that, on occasion, social media and other websites can have a dark side

The concept of privacy is dynamic and continues to change with the times of the day. Many scholars have tried to define privacy but there is currently no internationally accepted definition of privacy.

Privacy is a sweeping concept, encompassing inter alia freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations.

In the digital age, privacy has close nexus with data protection, data security, and surveillance. With the emergence of new technologies like Social media, artificial intelligence, and big data; new concepts of privacy like 'Privacy by Design', 'Privacy by Default', and 'Intellectual privacy' are evolved.

Chapter III contains a systematic analysis of privacy policies of Social Networking Sites/Apps.

Every social media website has a privacy policy. The purpose of a privacy policy is to outline how organizations will collect, maintain, and share user data. Often

organizations write the privacy policy in a way that protects the organization more than the user.[1]

Privacy policies are difficult to understand and contain ambiguous language that leaves out relevant information or contain words that leave statements made in the privacy policy open to interpretation.[2] Furthermore, privacy policies tend to be long boring documents with ambiguous and misleading language. Multiple studies in privacy policy readability found that although privacy policies are the only means for an organization to communicate data sharing and collection policies, the ambiguous, vague, and confusing language used undermines the effectiveness and purpose of the privacy policy.[3]

Another issue with privacy policies is that most users do not read them. Although young people claim, or appear to be, both concerned about and aware of privacy issues, they usually do not take any precautionary measures to protect themselves.[4]

Another privacy issue associated with social media is the use of targeted advertising. The corporate web platform operators and their third-party advertising clients continuously monitor and record personal data and online activities of the users. They store, merge and analyse collected data. This allows them to create detailed user profiles and to know a lot about the users' personal interests and online behaviours. Social media that are based on targeted advertising sell prosumers as a commodity to advertising clients. There is an exchange of money for access to user data that allows economic user surveillance.

Further, the researcher has discussed some controversial features of Facebook, Twitter and Google's products.

Facebook by its very nature, raises fundamental privacy challenges because it enables users to disclose unprecedented volumes of highly personal information, not only to friends and friends of friends, but, depending on one's privacy settings, to very large and unfamiliar audiences as well.

**News Feed,** a feature of Facebook that created a stream of headlines sent to all users based on the activities of their friends throughout the day including newly

[1]A. W. Haynes, "Online privacy policies: Contracting away control over personal information" *Penn State Law Review* 111, 587 (2007).
[2] Julie J. Beyer, *Privacy: The endangered species of the digital era* 81 (Faculty of Utica College, ProQuest LLC, 2018).
[3] *Id.* at 22.
[4] Monroe E. Price, Stefaan G. Verhulst, *et.al.* (eds.), *Routledge Handbook of Media Law* 476 (Routledge, New York, 2013).

uploaded pictures, changes in relationships, and so on. Due to controversial privacy issues of News Feed, Facebook CEO Mark Zuckerberg had to release an open letter apologizing to users for failing to build in privacy controls from the outset, which Facebook promptly corrected by introducing new controls.[5]

A year later, Facebook released **Beacon**, an addition to their developing ad platform. Beacon provided targeted ads based on items a user purchased or browsed on the websites of some forty-four partner sites and shared this information with a user's friends via the News Feed. Commentators labelled Beacon "a privacy disaster waiting to happen". Facebook discontinued Beacon in 2009 after settling a class-action lawsuit for $9.5 million.[6]

In 2007, Facebook launched the **Facebook Platform, a set of Application programming interfaces** ("APIs") and tools enabling developer to create hundreds of thousands of third-party applications ("apps") for Facebook users. Once approved by Facebook, apps may retrieve or post information to member profiles and request information about users and their friends. Canadian privacy regulators found that Facebook lacked adequate safeguards effectively restricting outside developers from accessing a user's profile information,[7] and called for technological measures restricting access to the information that was actually required to run a specific application.

Facebook uses **Facial Recognition Technology** (FRT) to identify people through their faces. Europe ordered Facebook to discontinue the use of facial recognition for photo tagging.[8] Many, including privacy groups and government agencies, have asserted several privacy concerns about the commercial use of FRT.

Google dominates the Internet with its products and services including its email service Gmail, video-sharing service YouTube, blogging platform Blogger, social media network Google+, and file-sharing service Google Drive. Google manages the most popular Internet search engine, which generates revenue when users click or view advertising related to their searches. The company has a long history of privacy issues.

---

[5] Ira S. Rubinstein and Nathaniel Good, "Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents" 28 (2) *Berkeley Technology Law Journal* 1393 (2013). DOI: https://www.jstor.org/stable/24119897

[6] *Id.* at 1394.

[7] *Id.* at 1395.

[8] JD Christopher T. Anglim (ed.), *Privacy Rights in the Digital Age* 190 (Grey House Publishing, USA, 2015).

**Gmail** is Google's free email service. Gmail's ad engine automatically scans header information and the content of incoming and outgoing messages for keywords provided by advertisers in advance. Despite privacy-sensitive design, Google's decision to fund free storage by serving contextual ads proved quite controversial.

Unlike Gmail, **Google Search** attracted more sustained interest from privacy officials. In 2006, European and U.S. regulators challenged Google and its search engine competitors regarding the amount, sensitivity, and retention periods of the data collected for search ads and other purposes. With Search, the public grew alarmed when it learned that leading search engines were tracking their searches and collecting and storing sufficient information.

**Google Street View** has been particularly controversial since inception of its launch. Street View allows users to view panoramic photographic images of locations and to zoom in and out on specific locations. Lauren H. Rakower, has argued that Street View violates the international right to privacy as stated by the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.[9]

On February 9, 2010, Google launched **Buzz**. Buzz included a feature that, "without prior notice or the opportunity to consent, Gmail users were, in many instances, automatically set up with 'followers' (people following the user)." Buzz raised multiple privacy concerns that brought about its untimely demise. Buzz violated several FIPs and related privacy engineering requirements, including inadequate and misleading notice and lack of informed consent.

On the basis of the above findings and discussion, the researcher found that "Privacy policies of social media are ambiguous, coercive and deceptive".

Chapter IV is an attempt to discuss in detail the legal framework of privacy laws in the context of social media worldwide.

One of the most controversial issues in relation to social media websites is their data processing and respect for privacy and personal data.[10] In the modern age data protection is a tool of privacy protection.[11] Data privacy laws essentially comprise a set of enforceable data privacy principles based on the 'life cycle' of personal data

[9] *Id.* at 248.
[10] Dr. Paul Lambert, *A User's Guide to Data Protection* 557 (Bloomsbury Professional Ltd, RH, 2016).
[11] Laura Scaife, *"Handbook of Social Media and the Law* 240 (Informa Law from Routledge, New York, 2015).

(collection, accuracy, security, use, disclosure, access, deletion etc.) coupled with an enforcement structure backed by legal measures requiring compliance.[12]

In 1972, the UK Government set up the Younger Committee. The report recommended ten principles for the use of computers for the processing of personal data - the forerunners of the present 'data protection principles.'

The Organization for Economic Co-operation and Development (OECD) Privacy Guidelines (1980) were an early influence on the development of data privacy laws. The OECD Guidelines on *the Protection of Privacy and Transborder Flow of Personal Data* were one of the first formulations of a comprehensive set of information privacy principles.[13]

Eight principles, namely Collection Limitation Principle, Data Quality Principle, Purpose Specification Principle, Use Limitation Principle, Security Safeguards Principle, Openness Principle, Individual Participation Principle, and Accountability Principle, were also adopted by the Organization for Economic Cooperation and Development (OECD) in order to regulate the trans-border data flow.

In 1984, The Data Protection Act, of UK established new rights for individuals to know if an organization was processing personal data about them and the right to have a copy of the information.

The Directive 95/46/EC of the European Parliament and of the Council was passed to balance the free flow of personal data within European Union member countries and the right to privacy of the European citizens. The directive prohibited the transfer of the individuals' information to a third country who doesn't have an adequate law on privacy protections.[14]

Considering the implications of the new technologies, the European Commission concluded that the Directive of 1995 needed to be amended and updated.

---

[12] Graham Greenleaf, *Asian Data Privacy Laws – Trade and Human Rights Perspective* 5-6 (Oxford University Press, United Kingdom, 2014).
[13] *Ibid.*
[14] Article 25 of Directive 95/46/EC of the European Parliament and of the Council, *The protection of individuals with regard to the processing of personal data and on the free movement of such data* (October 24, 1995). *available at*: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML (last visited on May 30, 2022).

On May 25th, 2018, the European Data Protection Regulation came into effect in order to harmonize data privacy laws across Europe.[15] This regulation replaced the Data Protection Directive of 1995.

EU GDPR covers social media provisions including data protection principles, consent issues, rights of data subjects, jurisdiction etc.

It is well established in human rights law that private entities are also equally responsible for protecting human rights and freedoms against unlawful interference by State and non-State actors. Companies should adhere to the "Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework".[16]

In order to be consistent with international human rights law, an interference with a qualified right such as privacy must meet the tests of legality, necessity, and proportionality.[17]

Since the Snowden revelations of mass surveillance in 2013, the United Nations (U.N.) General Assembly and U.N. Human Rights Council have considered resolutions on "the right to privacy in the digital age" every year, each taking turns to pass the text biennially.[18]

The report on **'**The Right to Privacy in the Digital Age 2014," recommended that States should review their own national laws, policies, and practices to ensure full conformity with international human rights law.[19]

The human rights council in march 2015, recalled that business enterprises have a responsibility to respect human rights as set out in the Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework.

---

[15] General Data Protection Regulation (GDPR). *available at*: https://gdpr-info.eu/ (last visited on May 30, 2022).

[16] UN General Assembly, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework,* UN Doc. A/HRC/17/31 p. 24 (March 21, 2011). *available at*: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G11/121/90/PDF/G1112190.pdf?OpenElement (last visited on May 30, 2022).

[17] Molly K. Land and Jay D. Aronson (eds), *New Technologies for Human Rights Law and Practice* 225-226 (Cambridge University Press, New Delhi, 2018).

**[18]** UN: To protect privacy in the digital age, world governments can and must do more, available at: https://www.article19.org/resources/un-to-protect-privacy-in-the-digital-age-world-governments-can-and-must-do-more/ (last visited on May 30, 2022).

[19] UN General Assembly*, The right to privacy in the digital age,* GA Res 27/37, GAOR, UN Doc A/HRC/27/37 (June 30, 2014). *available at*: http://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc (last visited on May 30, 2022).

Human Right Council on March 23, 2017 in its resolution no. 34/7 shows it concerns that "automatic processing of personal data for individual profiling may lead to discrimination or decisions that otherwise have the potential to affect the enjoyment of human rights. The council recalls that "States should ensure that any interference with the right to privacy is consistent with the principles of legality, necessity and proportionality."

UN General Assembly on 16 December, 2020 in its resolution 75/176 shows it concerns "about the spread of disinformation and misinformation, particularly on social media platforms, which can be designed and implemented so as to mislead, to spread racism, xenophobia, negative stereotyping and stigmatization, to violate and abuse human rights, including the right to privacy. Assembly calls upon all states *inter alia* "to consider developing or maintaining and implementing legislation, regulations and policies to ensure that all business enterprises, including social media enterprises and other online platforms, fully respect the right to privacy and other relevant human rights in the design, development, deployment and evaluation of technologies, including artificial intelligence, and to provide individuals whose rights may have been violated or abused with access to an effective remedy, including compensation and guarantees of non-repetition".[20]

The chapter concluded by drawing attention to the fact that although there are wide and continuous recommendations of the United Nations to protect "the right to privacy in the digital age" by the states as well as business enterprises but there is a huge implementation gap at the national level and by the business enterprises.

Chapter V is devoted to legal framework of privacy in context of social media in Indian perspective.

India does not have any specific data protection mechanism. Statutory protection of privacy can be found in India is scattered across a number of statutes. The Information Technology Act 2000 (IT Act), as amended by the Information Technology (Amendment) Act 2008 (ITAA), has the broadest scope.

The Protection of Human Rights Act 1993 (PHRA) defines 'human rights' by reference to India's obligations under its Constitution and international commitments,

[20] UN General Assembly, *The right to privacy in the digital age,* GA Res 75/176, GAOR, UN Doc A/RES/75/176 (December 16, 2020). a*vailable at:* https://documents-dds-ny.un.org/doc/UNDOC/GEN/N20/371/75/PDF/N2037175.pdf?OpenElement (last visited on May 30, 2022).

and is therefore broad enough to include ICCPR Article 17 concerning privacy[21]. It establishes the National Human Rights Commission (NHRC)[22] which has the power to investigate alleged violations[23] and can recommend that the government or authorities pay compensation, commence prosecutions, and approach courts for directions, orders, or writs. The NHRC has not had any major involvement in data privacy issues. No privacy issues are included in the hundreds of cases heard by it and summarized on its website since 1993.[24] Its focus has been, and is, on wrongful deaths and other extreme violations.

Section 79 of IT Act provides a balance between "technology necessity" and "legal necessity". The idea is to balance the rights of intermediaries within the legal framework, without disturbing the benefits accruing to the society at large from technological innovations.

Interception of any message or class of messages are regulated under the telegraph Act, 1885. However, a piquant situation arose with the coming into effect of the Information Technology Act, 2000, as under this Act, the Controller of Certifying Authorities had been given the mandate to intercept any information transmitted through any computer resource under section 69.

Over a period of time, blocking requests under section 69A have grown exponentially. Petitioners' increasingly invoking writ jurisdiction and even seeking removal of defamatory posts under section 69A. Surprisingly, the courts have so far been quite indulgent in this regard. In *Rahul@Biswajit Sinha v State of Bengal*[25], the Calcutta High Court directed not only removal of a news item as sought by the aggrieved petitioner but also ordered blocking of the online news portal called Biswa Bangla Sambad. However, in *Facebook Inc. v The State of West Bengal*[26] the Kolkatta High Court stayed the order of the Chief Metropolitan Magistrate, Kolkatta issued under section 69A. Blocking directions under section 69A has been sought to (a) ban PUBG online game[27]; and (b) ban the use of Zoom applications for official and personal

[21] Protection of Human Rights Act (India), s. 1(d).
[22] *Supra* note 21, s. 3.
[23] *Supra* note 21, s. 12(a).
[24] NHRC website www.nhrc.nic.in, See 'Human Rights cases' and 'Suo-Motu Cases'.
[25] *Rahul@Biswajit Sinha v. State of Bengal*, W.P. No. 4483(W) of 2018.
[26] *Facebook Inc. v. The State of West Bengal*, C.R.R. No. 2332 of 2017.
[27] *PIL No. 3 of 2019, Jammu & Kashmir*, High Court (Srinagar Branch).

purposes by the public[28]. Blocking of websites under section 69A has also been challenged[29].

On June 29, 2020 the Government of India banned 59 apps of Chinese origin[30], invoking powers under Section 69A of the Information Technology Act read with relevant provisions of the Information Technology (Procedure and Safeguards for Blocking of Access of Information by Public) Rules, 2009. The rationale behind banning these apps was data security, security and national sovereignty concerns. These apps include as TikTok, SHAREIt, UC Browser, CamScanner, Helo, Weibo, WeChat and Club Factory etc.

The right to privacy, before *Puttaswamy case*[31] derived its ambiguous basis from the right to life and personal liberty, as enshrined in Article 21.

On 24 August 2017, a Constitutional Bench of nine judges of the Supreme Court of India in ***Justice K.S. Puttaswamy (Retd.) v UOI*** *(supra)* upheld that Privacy is a Fundamental Right, which entrenched in Article 21 [Right to Life & Liberty]. It was held that

This landmark judgment fundamentally changed the way in which the government viewed its citizens' privacy, both in practice and prescription. Various steps have been taken by the Government of India to strengthen privacy regime. Government of India appointed a committee of experts for Data protection under the chairmanship of Justice B N Srikrishna that submitted its report[32] in July 2018 along with a draft Data Protection Bill[33]. The Report has a wide range of recommendations to strengthen privacy law in India.

The personal data protection bill, 2019 emphasized as the right to privacy is a fundamental right so it is necessary to protect personal data as an essential facet of information privacy. Chapter II of aforesaid bill talks about 'Obligation of Data Fiduciary' which includes different data protection principles adopted by the world

[28] *Harsh Chugh v. UOI*, WP© No. 10980 of 2020 presently pending before the Delhi High Court.
[29] *Tanul Thakur v. UOI*, Writ Petition No. 13037 of 2017 presently pending before the Delhi High Court.
[30] Press release issued by The Ministry of Electronics and information Technology, Government of India, *available at:* https://www.pib.gov.in/PressReleseDetailm.aspx?PRID=1635206 (last visited on May 30, 2022).
[31] *Justice (Retd.) K.S. Puttaswamy v. Union of India* (2017) 10 SCC 1.
[32] B. N. Srikrishna *available at:* https://en.wikipedia.org/wiki/B._N._Srikrishna (last visited on May 30, 2022).
[33] https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf (last visited on May 30, 2022).

community in their legislation. Chapter III talks about grounds for processing of personal data when consent is not required. Chapter IV talks about personal data and sensitive personal data of children. Chapter V highlights rights of data principal. Chapter VI deals with transparency and accountability measures to be taken by data fiduciary. Chapter VII prohibits transfer of personal data outside India.

New Social Media Rules 2021[34] has subsequently been passed to prescribe a code of ethics for online news, OTT platforms, and digital media. It indicates that the Right to Privacy is a matter of great concern in the phase of digitalization.

On October 27th, 2021 in Manohar Lal Sharma v Union of India & Ors,[35] also known as the Pegasus case, the Apex Court set up a Committee to examine the "spyware suite" Pegasus. "The Court has approached the issue as one that raises an "Orwellian concern", (about the alleged possibility of utilizing modern technology to hear what you hear, see what you see and to know what you do.) recognizing that intrusive surveillance not only violates the right to privacy but also has a chilling effect on freedom of speech and expression. Privacy is not the singular concern of journalists or social activists. Every citizen of India ought to be protected against violations of privacy…."

(This issue has highlighted that right to privacy can be in danger in the digital world if no effective measures are taken.)

In this chapter it is acknowledged that despite all international obligations of India, recommendation given by United Nations as well as Puttaswamy Constitutional Bench decision to enact data protection law, Government of India has still lot of work to be done to achieve the aspirations of these organizations.

On the basis of the discussion in Chapter IV: Privacy Laws & Social Media: International Perspective and Chapter V: Privacy Laws & Social Media: Indian Perspective, the researcher has found that one of the reasons for privacy violations of users in India is the lack of proper law in this regard.

Chapter VI contains information about the empirical study area, collection and analysis of data, interpretation and results. The purpose of this chapter is to examine, interpretate and critically evaluate information gathered from social media users and authorities (central universities in U.P.) to achieve the objectives of present study. This

[34] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
[35] 2021 SCC OnLine SC 985.

chapter is the heart of the whole of the research work. Through textual discussion, tabular and graphs, the data is critically analyses and reported along with the findings. Some of the important findings of chapter VI is as follows:

- Respondents of the youngest age are more addicted to social networking sites and apps.
- Survey shows that males are dominating in social media activities in comparison to females.
- Data shows that WhatsApp (16.8%) is the first choice of respondents followed by YouTube (15.0%) is the second choice while Facebook (14.1%) and Google (14.1%) are the third choice of respondents.
- Data (Table 6.30) show that 14.8% respondents perceive bodily privacy, communication privacy, informational privacy, territorial privacy as whole. 0.7% respondents replied that none of the options is a part of privacy. It reflects that respondents are not much aware about privacy concepts.
- Data (Table 6.32) shows that Only 14.3% respondents perceive informational privacy in consonance with Prof. Alan Westin view on informational privacy. Hence, awareness about informational privacy in the era of social media among social media users is not satisfactory.
- Social Media sites and apps are collecting users' information through overt and covert means. The researcher found in a survey (Table 6.34) that the awareness level of respondents about different types of information collected by SNSs/Apps is very low. Only 9.6% respondents have the perception that all kinds of information i.e., account information, contact information, payment information, location information, device information is collected by social networking sites and apps.
- Table 6.36 indicates that only 11.6% respondents have the perception that SNSs/Apps collect personal information of users for advertisement purposes, to provide better services, to develop new services, to share with law agencies on demand. Hence the awareness level of respondents about the purpose for which personal data of respondents is collected by SNSs/Apps is not satisfactory.
- Through a survey the researcher found that (Table 6.39 and Figure 6.40) that majority of the respondents 55.8% do not read privacy policies/ Terms and

Conditions of social networking sites / apps. This is alarming situation among respondents that they are not showing concerns towards privacy.

- Survey (Table 6.43 and Figure 6.44) shows that 13.2% respondents do not concern about privacy of personal information on social media, 31.5% respondents specify settings, 34.7% respondents are concerned about personal information but still share personal information, 19.3% respondents shown their concern, hence they don't share their personal information. Hence, it has been found that the level of privacy concern among respondents is not satisfactory.
- The researcher found (Table 6.50) that only 13.8% respondents are aware about data subjects rights while the remaining respondents are partially aware about data subjects rights. Hence, awareness about data subject rights among respondents is not satisfactory.
- Table 6.58 shows that only 13.4% respondents have expressed their view that while processing personal data all data protection principles (fair & lawful, purpose limitation, data quality, data security) must be kept in mind by the SNSs/Apps. Hence, it shows that awareness about data protection principles among respondents is not satisfactory.
- The researcher found that (as Table 6.61 and Figure 6.62 reveal) majority of the respondents (57.2%) did not participate in any privacy/cyber issues awareness programmes, only 28.5% respondents participated in a privacy/cyber issues awareness programme organized by concerned university while as 12.5% respondents are not aware about such programmes.
- The researcher found that privacy concerns of central universities in Uttar Pradesh are not satisfactory. Out of six universities only Aligarh Muslim University, Aligarh and Banaras Hindu University, Varanasi responded to the queries of the researcher.
- The researcher found that university is mostly dependent on social networking sites / apps for imparting education. They don't have their own software.
- The non-responsive nature of universities depicts that no university (considered in research work) is taking any measures to protect the personal data of students, teaching staffs and non-teaching staffs to protect, respect the right to privacy of concerned persons.

- The survey shows that programmes organized by universities to make students aware about privacy/cyber related issues is negligible.

The researcher on the basis of above findings reached the conclusion that "awareness regarding legal provisions and privacy policies of social media among the students of central universities in Uttar Pradesh is not adequate". Hence, the hypothesis "awareness regarding legal provisions and privacy policies of social media among the students of central universities in Uttar Pradesh is not adequate" is proved.

## SUGGESTIONS

**1.** There are large gaps in our knowledge, research and understanding of developing issues in social media platform. More research is needed to appraise ourselves of all potential solutions and policy decisions as well as assisting websites to fully engage their own (corporate, moral and legal) responsibilities and functional capabilities.

**2.** Effective remedy against the violation of privacy can be a reality only when the law considers the context of the time. A flexible yet robust privacy protection regime in India is the need of today.

**3.** The ubiquitous nature of data in our present day has generated progress but at the same time there is a need for the law to respond to this progress by protecting vulnerable rights of citizens.

**4.** The legal framework must also consider that with the augmentation of technology, communication privacy is endangered by private and State actors. Therefore, devising a framework that has procedural safeguards and ensure credible communication security is the need of the hour.

**5.** Given the right kind of government, the state can also pass legislation that protects consumers' and employees' privacy form surveillance that serves corporate interests. The state, for example, has the power to potentially ban or considerably limit all workplace surveillance and consumer surveillance, and to thereby strengthen privacy rights. This requires, however, consumer- and worker-oriented politics.

**6.** More work needs to be done to capitalize on the benefits of digital technologies to advance human rights — while ensuring that these same technologies do not infringe on them. Human Rights is a good model to build upon in order for

governments, industry, and civil society to protect rights while reaping the benefits of digital technologies.

7. Interception of communication in the current geopolitical environment is often necessary in the interest of national security. Therefore, there is a requirement for the law to balance security interests with the right to privacy in the sphere of communication.
8. To protect our privacy in digital age we need to know the value of our personal information that we share online and other aspects like who is gathering data about us, how that data is used by whom, who can hold that data, how can we delete our personal data and so forth.
9. There is a need to make people socially and legally aware of right perception of privacy, privacy as a legal and human right, rights of data subjects, and remedies available in case of online violation of privacy in the context of social media.
10. State, civil societies, higher educational institutions and others can play a major role in spreading awareness among users to protect privacy in social media platform.

**RECOMMENDATIONS SPECIFIC TO THE STATE**

I. The State must respect and protect the right to privacy, including in the context of digital communications.
II. The State should take all measures to put an end to violations of the right to privacy and to create the conditions to prevent such violations, including by ensuring that relevant national legislation complies with its obligations under international human rights law.
III. The State must review, on a regular basis, their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law.
IV. The State must provide individuals whose right to privacy has been violated by unlawful or arbitrary surveillance with easy access to an effective remedy, consistent with international human rights obligations.
V. The State should consider developing or maintaining and implementing adequate legislation, in consultation with all relevant stakeholders, including

business enterprises, international organizations and civil society, with effective sanctions and appropriate remedies, that protects individuals against violations and abuses of the right to privacy, namely through the unlawful and arbitrary collection, processing, retention, sharing or use of personal data by individuals, Governments, business enterprises and private organizations;

**VI.** The State should consider developing or maintaining and implementing legislation, regulations and policies to ensure that all business enterprises, including social media enterprises and other online platforms, fully respect the right to privacy and other relevant human rights in the design, development, deployment and evaluation of technologies, including artificial intelligence, and to provide individuals whose rights may have been violated or abused with access to an effective remedy, including compensation and guarantees of non-repetition.

**VII.** The State must consider adopting or maintaining data protection legislation, regulation and policies, including on digital communication data, that comply with their international human rights obligations, which could include the establishment of national independent authorities with powers and resources to monitor data privacy practices, investigate violations and abuses and receive communications from individuals and organizations, and to provide appropriate remedies;

**VIII.** The State must provide effective and up-to-date guidance to business enterprises on how to respect human rights by advising on appropriate methods, including human rights due diligence.

**IX.** The State must promote quality education and lifelong educational opportunities for all to foster, inter alia, digital literacy and technical skills to effectively protect their privacy.

**RECOMMENDATIONS SPECIFIC TO BUSINESS ENTERPRISES INCLUDING SOCIAL MEDIA**

**A.** All business enterprises that collect, store, use, share and process data of users must respect human rights in accordance with the Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework.

**B.** Social Media must inform users in a clear and easily accessible way about the collection, use, sharing and retention of their data that may affect their right to privacy and to establish transparency policies that allow for the free, informed and meaningful consent of users, as appropriate.

**C.** Social Media must implement administrative, technical and physical safeguards to ensure that data are processed lawfully and to ensure that such processing is limited to what is necessary in relation to the purposes of the processing and that the legitimacy of such purposes, as well as the accuracy, integrity and confidentiality of the processing, is ensured.

**D.** Social media must ensure that respect for the right to privacy and other international human rights is incorporated into the design, operation, evaluation and regulation of automated decision-making and machine-learning technologies and to provide for compensation for the human rights abuses that they may cause or to which they may contribute.

**E.** Social Media must provide individuals easy mechanisms to access to their personal data and to adopt appropriate measures for the possibility to amend, correct, update, delete and withdraw consent for the data, in particular if the data are incorrect or inaccurate, or if the data were obtained illegally.

**F.** Social Media must put in place adequate safeguards that seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services, including where necessary through contractual clauses or notification of any relevant entities of abuses or violations when misuse of their products and services is detected.

**RECOMMENDATIONS SPECIFIC TO HIGHER EDUCATIONAL INSTITUTIONS**

**a.** Higher Educational Institutions must adopt mechanisms to respect and protect the right to privacy of students, staff (academic and non-academic).

**b.** Higher educational institutions must adopt privacy policies (the ways in which collect, store, use, share and process data of users) on their websites and apps.

**c.** Higher educational institutions must constitute a body whose task must to issue guidelines to different departments to use safer Internet practices, using education tools for imparting education free from privacy violations.

**d.** Higher educational institutions must consider to develop their own software for online teaching with the coordination of the legal department, IT department, and other appropriate departments of the institute.

**RECOMMENDATIONS SPECIFIC TO THE SPREAD OF PRIVACY AWARENESS/LITERACY**

a) The students must understand the value of their personal information disseminated via social media. Only Least necessary information must be shared with social media.

b) The students must read the privacy policies of social media during and later the registration process and act accordingly.

c) Higher educational institutions and civil society must engage in the spread of privacy awareness through seminars, conferences, and symposiums.

# BIBLIOGRAPHY

# BIBLIOGRAPHY


## INTERNATIONAL CONVENTIONS/ DECLARATION/ STATUTES

- Universal Declaration of Human Rights, 1948
- United Nations Charter, 1945
- International Covenant on Civil and Political Rights, 1966
- International Covenant on Economic, Social and Cultural Rights, 1966
- International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families, 1990
- European Convention on Human Rights, 1953
- American Convention on Human Rights, 1979
- African Charter of Human and People's Rights, 1979

## INTERNATIONAL LEGISLATIONS / ACTS/ STATUTES

- The OECD Guidelines, 1980
- Data Protection Act, 1984
- The General Data Protection Directive 95/46/EC
- Data Protection Act, 1998
- Data Protection Act, 2018
- EU General Data Protection Regulation, 2018

## NATIONAL LEGISLATIONS / ACTS/ STATUTES

- The Constitution of India, 1950
- The Credit Information Companies (Regulation) Act, 2005
- The Indian Contract Act, 1872
- The Indian Penal Code, 1860
- The Indian Telegraph Act, 1885

- The Information Technology Act, 2000
- The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
- The Protection of Human Rights Act, 1993
- The Recovery of Debts Due to Banks and Financial Institutions Act, 1993
- The Specific Relief Act, 1963

**BOOKS**


1. Alan Westin, Privacy and Freedom (IG Publishing, New York, 1967).
2. Bernal Paul, Internet Privacy Rights – Rights to Protect Autonomy (Cambridge University Press, United Kingdom, 2014).
3. Brian D. Loader & Dan Mercea (ed.), Social Media and Democracy, (Routledge, 2012).
4. Christian Fuchs, Social Media a critical introduction (Sage Publications India Pvt Ltd, New Delhi, 2017).
5. C. R. Kothari, Research Methodology Methods and Techniques, (New Age International Publishers, 2004).
6. Daniel J. Solove, The Digital Person Technology and Privacy in the Information Age, (New York University Press, New York, 2004).
7. Daniel J. Solove, Understanding Privacy (Harvard University Press, USA, 2008).
8. David Rainbridge, Data Protection Law (Universal Law Publishing Co. Pvt. Ltd., Delhi, 2007).
9. Daxton R. Stewart, (Ed.) Social Media and the Law A Guidebook for communications Students and Professionals (Routledge, New York, 2017).
10. Dr. Majid Reza Momeny, The United Nations in the Era of Globalization (K.K. Publications, New Delhi, 2013).

**11.** Dr. Paul Lambert, A User's Guide to Data Protection (Bloomsbury Professional Ltd, RH, 2016).

**12.** Dr. S. R. Myneni, Legal Research Methodology, (Allahabad Law Agency, Allahabad, 2013).

**13.** Dr. S. V. Joga Rao, Law of Cyber Crimes & Information Technology Law (Lexis Nexis Butterworth Wadhwa, Nagpur, 2nd ed., 2009).

**14.** Dr. U. Chandra, Human Rights (Allahabad Law Agency Publication, 7th edn., 2007).

**15.** Durga Das Basu, Human Rights in Constitutional Law: Along with International Human Rights Documents (Lexis Nexis Butterworths, Wadhwa Nagpur, 3rd edn., 2008)

**16.** Ferdinand David Schoeman, Philosophical Dimensions of Privacy – An Anthology (Cambridge University Press, Cambridge, 1984).

**17.** Graham Greenleaf, Asian Data Privacy Laws – Trade and Human Rights Perspective (Oxford University Press, United Kingdom, 2014).

**18.** H. O. Agarwal, International Law & Human Rights (Central Law Publication, 13th edn., 2006).

**19.** Janice Richardson, Law and the Philosophy of Privacy (Routledge, New York, 2016).

**20.** JD Christopher T. Anglim (ed.), Privacy Rights in the Digital Age (Grey House Publishing, USA, 2015).

**21.** John Allen, Online Privacy and Hacking (Reference Point Press, US, 2015).

**22.** John W. Creswell, Research Design, Qualitative, Quantitative, and Mixed Method of Approaches, (Sage Publications, 2014).

**23.** Kiran Deshta, Right to Privacy under Indian Law (Deep & Deep Publications Pvt. Ltd., New Delhi, 2011).

**24.** Laura Scaife, Handbook of Social Media and the Law (Informa Law from Routledge, New York, 2015).

**25.** Lee A. Bygrave, Data Privacy Law An International Perspective, (Oxford University Press, United Kingdom, 2014).

**26.** Lyombe S. Eko, New Media Old Regimes (Lexington Books, U.K., 2012).

**27.** M.P. Jain, Indian Constitution Law (Lexis Nexis, 8th ed., Reprint 2022).

**28.** Molly K. Land and Jay D. Aronson (eds.), New Technologies for Human Rights Law and Practice (Cambridge University Press, New Delhi, 2018).

**29.** Monroe E. Price, Stefaan G. Verhulst and Libby Morgan et.al. (eds.), Routledge Handbook of Media Law (Routledge, New York, 2013).

**30.** Neil Richards, Intellectual Privacy Rethinking Civil Liberties in the Digital Age (Oxford University Press, New Delhi, 2015).

**31.** Neil Richards, Why Privacy Matters (Oxford University Press, UK, 2022).

**32.** Normann Witzleb, David Lindsay, Moira Paterson, Sharon Rodrick (ed.), Emerging Challenges in Privacy Law (Cambridge University Press, Cambridge, 2014).

**33.** Pawan Duggal, Cyber Law, (Universal Law Publishers, 2022).

**34.** P. M. Bakshi, The Constitution of India (Universal Lexis Nexis, 18th ed., 2022).

**35.** Ram Jethmalani and D. S. Chopra, Cases and Material on Media Law (Thomson Reuters, New Delhi, 2012).

**36.** Raymond Wacks, Privacy a Very Short Introduction (Oxford University Press, Oxford, 2010).

**37.** Richard A. Posner, The Economics of Justice (Harvard University Press, Cambridge, 1981).

**38.** S. R. Chauhan and N.S. Chauhan (eds.), International Dimensions of the Human Rights (Global Vision Publishing House, New Delhi, 2006).

**39.** Sam Hinton & Larissa Hjorth, Understanding Social Media (Sage Publications, New Delhi, 2013).

**40.** Siva Vaidhyanathan, Antisocial Media – How Facebook Disconnects Us and Undermines Democracy (Oxford University Press, New York, 2018).

**41.** Stefan-Ludwig Hoffman, Human Rights in Twentieth-Century (Cambridge University Press, Cambridge, 2011).

**42.** Stephen Currie, How is the Internet eroding the privacy rights (Reference Point Press, 2014).

**43.** Upendra Baxi, The Future of Human Rights (Oxford University Press, New Delhi, 3rd ed., 2008).

**44.** V. N. Viswanathan, Human Rights Challenges of 21st Century (Kalpaz Publications, Delhi, 2009).

**45.** Vakul Sharma and Seema Sharma, Information Technology Law and Practices (Universal LexisNexis, India, 7th Edition, 2021).

**46.** Varinder Taprial & Priyanka Kanwar, Understanding Social Media, (Ventus Publishing ApS, 2012).

## ARTICLES

**1.** A. W. Haynes, Online privacy policies: Contracting away control over personal information, *Penn State Law Review* (2007).

**2.** Adam D. Moore, Privacy: Its Meaning and Value, *American Philosophical Quarterly*, Vol. 40, No. 3 (Jul., 2003).

**3.** Andrei Marmor, What Is the Right to Privacy, *Philosophy & Public Affairs,* Vol. 43, No. 1 (WINTER 2015).

**4.** Alessandro Acquisti, Curtis Taylor and Liad Wagman, The Economics of Privacy, *Journal of Economic Literature,* Vol. 54, No. 2 (June, 2016).

**5.** Anja Bechmann, Non-Informed Consent Cultures: Privacy Policies and App Contracts on Facebook, *Journal of Media Business Studies* (16 Mar, 2015).

**6.** Bhairav Acharya, The Four Parts of Privacy in India, *Economic and Political Weekly*, Vol. 50, No. 22 (May 30, 2015).

**7.** Charles Fried, Privacy, *The Yale Law Journal,* Vol. 77, No. 3 (1968).

**8.** D.M. Boyd and N.B. Ellison, Social network sites: definition, history and scholarship, *Journal of Computer-Mediated Communication,* Vol. 13 No. 1 (2007).

**9.** David J. Kessler, Sue Ross and Elonnai Hickok, A Comparative Analysis Of Indian Privacy Law And The Asia-Pacific Economic Cooperation Cross-Border Privacy Rules, *National Law School of* India Review, Vol. 26, No. 1 (2014).

**10.** E. L. Godkin, Libel and Its Legal Remedy, *Journal of Social Science,* Vol. 12 (1880).

**11.** Ferdinand Schoeman, Privacy: Philosophical Dimensions, *American Philosophical Quarterly*, Vol. 21, No. 3 (Jul., 1984).

**12.** Helen Nissenbaum, Protecting Privacy in an Information Age: The Problem of Privacy in Public, *Law and Philosophy,* Vol. 17, No. 5/6 (Nov., 1998).

**13.** Herman T. Tavani, Philosophical Theories of Privacy: Implications For an Adequate Online Privacy Policy, *Metaphilosophy* Vol. 38, No. 1 (January 2007).

**14.** Hyman Gross, The Concept of Privacy, *New York University Law Review,* Vol. 43 (1967).

**15.** Ira S. Rubinstein and Nathaniel Good, Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents, *Berkeley Technology Law Journal,* Vol. 28 No. 2 (2013).

**16.** Jed Rubenfeld, The Right of Privacy*, Harvard Law Review*, Vol. 102 (1989).

**17.** John R. Drake, Asking for Facebook Logins: An Egoist Case for Privacy, *Journal of Business Ethics*, Vol. 139, No. 3 (December 2016).

**18.** Herman T. Tavani, Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy, *Metaphilosophy*,Vol. 38, No. 1 (January 2007).

**19.** Jerry Kang, Information Privacy in Cyberspace Transactions, *Stanford Law Review,* Vol. 50 (1998).

**20.** Jordon Steele, Preserving History, Preserving Privacy: E-Mail, Archival Ethics, And the Law, *Archival Issues,* Vol. 32, No. 2 (2010).

**21.** Katayoun Baghai, Privacy as a Human Right: Sociological Theory, *Special Issue: The Sociology of Human Rights,* Vol. 46, No. 5, (October, 2012).

**22.** Kirsten Martin, Understanding Privacy Online: Development of a Social Contract Approach to Privacy, *Journal of Business Ethics*, Vol. 137, No. 3 (September 2016).

**23.** Kirsty Hughes, A Behavioural Understanding of Privacy and its Implications for Privacy Law, *The Modern Law Review,* Vol. 75, No. 5 (September 2012).

**24.** Norman E. Bowie and Karim Jamal, Privacy Rights on the Internet: Self-Regulation or Government Regulation?, *Business Ethics Quarterly,* Vol. 16, No. 3 (July, 2006).

**25.** Nuala O'Connor, Alethea Lange and Ali Lange, Privacy in the Digital Age, *Great Decisions,* (2015).

**26.** Özgür Heval Çınar, The current case law of the European Court of Human Rights on privacy: challenges in the digital age, *The International Journal of Human Rights* (2021).

**27.** Priti Saxena, Technological Advancements: Enriching or Violating Human Rights? *Journal Of The National Human Rights Commission, India* (December 10, 2021).

**28.** Robert E. Mensel, Kodakers Lying in Wait: Amateur Photography and the Right to Privacy in New York, *American Quarterly* (1991).

**29.** Ruth Gavison, Privacy and the Limits of Law, *The Yale Law Journal*, Vol. 89, No. 3 (Jan., 1980).

**30.** Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, *Harvard Law Review,* Vol. 4, No. 5. (Dec. 15, 1890).

**31.** Sarah Shik Lamdan, Social Media Privacy: A Rallying Cry to Librarians, *The Library Quarterly: Information, Community, Policy,* Vol. 85, No. 3 (July 2015).

**32.** Sidney M. Jourard, Some Psychological Aspects of Privacy, *Law and Contemporary Problems,* Vol. 31 (1966).

**33.** Tom Gerety, Redefining Privacy, *Harvard Civil Rights-Civil Liberties Law Review,* Vol. 12, No. 2 (1977).

**34.** William Prosser, Privacy, *California Law Review,* Vol. 48 (1960).

**35.** Wouter M. P. Steijn and Anton Vedder, Privacy under Construction: A Developmental Perspective on Privacy Perception, *Science, Technology, & Human Values,* Vol. 40, No. 4 (July 2015).

**Reports**

❖ Social Media for Youth & Civic Engagement in India, published Jointly by Ministry of Youth Affairs & Sports, UNV (United Nations Volunteer India) and UNDP (2019).

❖ Srikrishna Committee Report, Law Commission of India.

## WEBSITES


- https://www.academia.edu
- http://www.allduniv.ac.in
- http://www.amu.ac.in
- http://www.bbau.ac.in
- http://www.bhu.ac.in
- http://www.booksc.org
- http://europa.eu
- https://www.ec.europa.eu
- http://www.facebook.com
- https://gdpr-info.eu
- http://www.google.com
- http://www.thehindu.com
- http://www.jstor.org
- https://www.legislation.gov.uk
- http://www.livelaw.in
- http://www.main.sci.gov.in
- http://www.meity.gov.in
- http://www.ohchr.org
- http://www.rgnau.ac.in
- http://www.rlbcau.ac.in
- http://www.twitter.com
- https://www.un.org
- https://www.unhcr.org
- https://www.wikipedia.com

# APPENDICES

**Appendix - 1**

# QUESTIONNAIRE

**(For Social Media Users)**

**Dear Respondent!**

I am a research scholar, pursuing my Ph.D. in Human Rights from Babasaheb Bhimrao Ambedkar (Central) University, Lucknow (Uttar Pradesh) under the supervision of Prof. Preeti Misra (Supervisor) & Dr. Rashida Ather (Co-supervisor). My Research Topic is ***"Privacy as a Human Right in the Digital Age: A Socio-Legal Study of Social Media Users with Special Reference to Students of Central Universities in Uttar Pradesh".***

The purpose of this questionnaire is to collect the information of different social media users regarding the privacy issues. I therefore, humbly request you to kindly spare your valuable time and share your views by filling up the following questionnaire.

I assure you that all the information provided by you will be kept confidential and will be used for academic purpose only.

## PART – A

## Basic Information of Social Media Users

(Kindly Mark √ your answer, you may choose more than one options, where you feel appropriate)

**Q.1. Age Group**

a. 18 - 22
b. 23 - 26
c. 27 - 30
d. Above 30

**Q.2. Gender**

a. Male
b. Female
c. Transgender

**Q.3. Level of Course Pursuing**

a. Graduation
b. Postgraduation
c. M.Phil./Ph.D.
d. Other

**Q.4. To which university do you belong?**

a. Aligarh Muslim University, Aligarh (AMU)
b. Babasaheb Bhimrao Ambedkar University, Lucknow (BBAU)
c. Banaras Hindu University, Varanasi (BHU)
d. Rajiv Gandhi National Aviation University, Raebareli (RGNAU)
e. Rani Lakshmi Bai Central Agriculture University, Jhansi (RLBCAU)
f. University of Allahabad, Prayagraj (AU)

**Q.5. Which social networking sites (SNSs) /apps do you use most?**

a. Facebook
b. Instagram
c. WhatsApp
d. Google (Search Engine)
e. YouTube
f. Google Pay
g. Twitter
h. Wikipedia / WordPress
i. LinkedIn
j. Telegram
k. Others (……)

**Q.6. Does your university permit you to use social networking sites in your cyber library /computer lab?**

a. Yes b. No c. Sometimes d. Not Sure

**Q.7. What do you normally post in social media sites / Apps?**

a. Text messages b. Images c. Videos d. Links e. Others

**Q.8. For what purpose do you use social media?**

a. Communication
b. Education
c. Entertainment
d. Shopping
e. Finance
f. Gaming
g. Any Others (Please Specify …..)

## PART - B
## Privacy: Awareness & Attitude

**Q.9. When you hear the word privacy, what comes to your mind?**

a. Bodily privacy (i.e., your physical body)
b. Communication privacy (i.e., calls received or dialled through telephone)
c. Information privacy (i.e., information exchanged on the Internet)
d. Territorial privacy (i.e., your living space, working space)
e. All of the above
f. None of Above
g. Any Others (Please Specify ….)

**Q. 10. How informational privacy can be best described?**

a. Freedom from official intrusion
b. The right to respect for private life i.e., the right to be let alone
c. Key value which underpins human dignity
d. the security and privacy of mail, telephones, email, and other forms of communication
e. the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others
f. All

**Q. 11. What kind of personal information shared by you is collected by social networking sites /apps?**

a. Basic account information (name, e-mail id)
b. contact information and address books
c. payment information
d. location information
e. Device Information
f. All above
g. Don't Know

**Q.12. For what purpose social networking sites / apps do use your personal information?**

a. advertisement purpose
b. to build better services
c. to develop new services
d. to share with law enforcement agencies
e. All Above
f. Can't Say

**Q.13. Can you access any social networking sites /apps without allowing to access images, videos, recording of call, files to social networking sites/app?**

a. Yes b. No c. Sometimes d. Not sure

**Q.14. Do you read all the terms and conditions of social networking sites/Apps at the time of registration?**

a. Yes b. No c. Not sure

**Q. 15. Do you give expressed consent to SNSs/apps to share your personal information with third parties / advertisers?**

a. Yes b. No c. Not sure

**Q.16. How do you concern about privacy of your personal information on social media?**

a. Not concerned at all
b. Specified my settings, my data is secure
c. Concerned; but still share my personal information
d. Concerned; hence don't share personal information

**Q.17. How do you limit social networking sites / apps to collect your personal information?**

a. Specifies my settings
b. Using tools to object, restrict or withdraw consent
c. Removing and deleting personal information
d. Don't take any action

**Q. 18. How do you respond when new privacy policies of social networking sites /apps are notified and informed you at your mobile?**

a. Read privacy policy and act accordingly
b. Takes legal action accordingly if it violates basic data protection principles
c. Shows concern through writings in newspaper/blogs etc.
d. Doesn't care

## PART - C
## Privacy: Legal Awareness & Remedies

**Q.19. What are the rights of Data Subjects (Social Media Users)?**
a. Right to information (ability to ask a company about personal data being processed)
b. Right to access (ability to get access to his or her personal data)
c. Right to withdraw consent
c. Right to delete personal data
d. All the above
e. None of the above
f. Not sure

**Q.20. Right to Privacy is**
a. Fundamental Right in India
b. Basic Human Right
c. Both (Fundamental Right and Human Right)
c. Not Sure

**Q.21. Is Imposition and implementation of policy (like installation of Arogyasetu in your mobile) without proper legislation a violation of Human Right?**
a. Yes
b. No
c. Not Sure

**Q.22. Does Government of India have proper legislation to deal with protection of privacy of citizens in online social media?**
a. Yes
b. No
c. Not Sure

**Q.23. What do you expect from social networking sites and apps while processing of your personal data?**
a. Fair and lawful processing
b. Purpose Limitation (collect personal data for specific purpose)
c. Data quality (data collected should be relevant, accurate, and complete)
d. Data security (personal data should be protected against unauthorized attempts to disclose, delete, change, or exploit)
e. All above
f. None of Above

**Q.24. If your privacy is violated over social media platform, what action will you take for its protection?**
a. file injunction suit in court
b. file complaint in state/national human rights commission
c. file complaint before concerned authority
d. register FIR under a specific legislation
e. not take any action

**Q.25. Have you ever participated in any program organized by your university to spread awareness about privacy/cyber issues in online social media platform?**
a. Yes
b. No
c. Not aware about such programs

**Any Other Suggestion:** _____

**Signature** _____

**Name of the respondent**_____ **Mobile No.** (Optional)_____

**Please Return To:**
Shiv Kumar,
Research Scholar,
Department of Human Rights,
School of Legal Studies, BBAU
Mobile: 9868602158, 8587834021
Email: shivkumarrawat@gmail.com

**Thank you so much for sparing your precious time.**

**Appendix - 2**

**To,** Date: 20.12.2021

The CPIO,
Aligarh Muslim University,
Aligarh - 202002, U.P.

**Subject**: Seeking following information under RTI Act, 2005
**Fees**: Postal Order No. 56F 239414 is attached.

**Respected Sir/Madam,**

The applicant seeks following information. Humble request to furnish the same.

1. What kind of social networking sites and apps university is using for imparting online education or intercommunication with staffs?
   a. Googlemeet
   b. Zoom
   c. Webex
   d. Facebook
   e. Youtube
   f. Others ……..
2. Does university have its own software/apps used for online teaching & other purpose free from violation of privacy?
   (a) Yes
   (b) No
3. Is there any policy adopted by the University to protect personal information of students, research scholars, teaching staffs and non-teaching staff?
   (a) Yes
   (b) No
4. What measures is being taken between university and agencies (acting on behalf of university like National Testing agency and others) regarding the processing of personal information of concerned persons (students, teaching staffs, non-teaching staff) to respect, protect the right to privacy?
   (a) Have a MOU between University and agencies not to share personal data with others.
   (b) Delete data after reasonable time period, once purpose is fulfilled.
   (c) Seek consent of concerned persons regarding processing of data like uploading on website
5. Does your university's website www.amu.ac.in follow any privacy policies?
   a. Yes
   b. No
6. (a) Has any department of university organized privacy awareness program for students in context of social media?
   (b) If yes, how many such programs have been organized from January 2019 to January December 2021?

**Regards,**
Shiv Kumar,
Research Scholar,
Department of Human Rights,
School of Legal Studies,
Babasaheb Bhimrao Ambedkar (Central) University,
Vidya Vihar, Raebareli Road, Lucknow - 226025

**Appendix – 3A**

D.No.: R-22878/CC Dated: 27-12-2021

To,
Mr. Shiv Kumar,
Research Scholar,
Department of Human Rights,
School of Legal Studies,
Babasaheb Bhimrao Ambedkar (Central) University,
Vidya Vihar, Raebareli Road, Lucknow-226025

Kindly refer to your application received in CAPIO Office R.No. 656/CAPIO/F/21-22 dated 23.12.2021 addressed to CPIO, Aligarh Muslim University received by the Deputy Registrar (Legal) & CAPIO seeking some information in respect under RTI Act 2005 and CAPIO has transferred the RTI to CPIO Prof. M.N.Faruqui Computer Center (PMNFCC) vide R-22878/CC dated 24-12-21 to provide the reply of queries directly to the information seeker under RTI Act-2005. As CPIO, PMNFCC, asked for responses from the Webmaster, AMU website who is the proper person to get responses and links (if any) for the queries on 24-12-2021. **please find attached herewith the responses of your queries received from the Webmaster.** However, the query no. 4 is not related with PMNFCC, the proper response may be received from CPIO, Controller Office, therefore the **query no. 4 is being transferred to the CPIO, Controller Office, AMU under section 5(4) & 5(5) of RTI Act, 2005 to provide the desired information directly to the information seeker**.

If you are not satisfied with this reply may prefer appeal to the Appellate Authority.

Appellate Authority

**Director**
**Prof. M.N. Faruqui Computer Centre**
**Aligarh Muslim University**
**Aligarh**

27-12-2021
CPIO
Prof. M.N.Faruqui Computer Centre
AMU

**Copy to:**
1. **CPIO, Controller Office, AMU with the request to provide required information for Item 4 at your end directly to the information seeker under Section 5(4) & 5(5) of RTI Act, 2005.**
2. Deputy/Joint Registrar (Legal) & CAPIO for information

CPIO
Prof. M.N.Faruqui Computer Centre

**Encl.:**
1. Copy of RTI Application
2. Response of Queries received from the Webmaster, PMNFCC, AMU

**Appendix – 3B**

Please refer the RTI reference Number 656/CAPIO/F/21-22 dated 24-12-2021, the pointwise replies are as follows:

**Queries 1:** Multiple platforms including Google meet, Zoom, YouTube, Moodle LMS etc. are being used various Faculties, Departments, OUs as per the number of concurrent users in the class/session/online events and preference of the individual Faculties/Departments/Colleges /Institutes.

**Queries 2:** In addition to multiple secure online platforms mentioned at point number 1, University also has an on-premise institutional LMS (https://lms.amu.ac.in) which is made available at all faculty of studies for progressive adoption by all concern.

**Queries 3:** University has adopted IT Policy and guidelines, a copy of the same is available at public domain (https://api.amu.ac.in/storage/file/pdf/cc/ITP.pdf)

**Queries 4:** Item related to another office *Admissions and Examinations*, the matter may be referred to this office.

**Queries 5:** University has multiple websites maintained by respective computer cells like Computer Cell admissions and Examinations, Computer Cell Registrar's Office etc. Each of which is governed by IT Policy mentioned at point number 3. URL (www.amu.ac) is not correct however University is committed to respecting and following privacy.

**Queries 6:** Information seeker may like to peruse the university website where information may be available at multiple sections including departmental webpages (https://amu.ac.in/department-list), past events (https://amu.ac.in/events) and News Section (https://amu.ac.in/news) etc. in its quest for information.

Malik Hayat Hashmi
Systems Programmer and Webmaster
PMNF Computer Centre

**Appendix - 4**

**To,** Date: 20.12.2021

The CPIO,
Babasaheb Bhimrao Ambedkar (Central) University,
Vidya Vihar, Raebareli Road, Lucknow - 226025

**Subject**: Seeking following information under RTI Act, 2005
**Fees:** Postal Order No. 56F 239415 is attached.

**Respected Sir/Madam,**

The applicant seeks following information. Humble request to furnish the same.

1. What kind of social networking sites and apps university is using for imparting online education or intercommunication with staffs?
   a. Googlemeet
   b. Zoom
   c. Webex
   d. Facebook
   e. Youtube
   f. Others ……..
2. Does university have its own software/apps used for online teaching & other purpose free from violation of privacy?
   (a) Yes
   (b) No
3. Is there any policy adopted by the University to protect personal information of students, research scholars, teaching staffs and non-teaching staff?
   (a) Yes
   (b) No
4. What measures is being taken between university and agencies (acting on behalf of university like National Testing agency and others) regarding the processing of personal information of concerned persons (students, teaching staffs, non-teaching staff) to respect, protect the right to privacy?
   (a) Have a MOU between University and agencies not to share personal data with others.
   (b) Delete data after reasonable time period, once purpose is fulfilled.
   (c) Seek consent of concerned persons regarding processing of data like uploading on website
5. Does your university's website www.bbau.ac.in follow any privacy policies?
   a. Yes
   b. No
6. (a) Has any department of university organized privacy awareness program for students in context of social media?
   (b) If yes, how many such programs have been organized from January 2019 to January December 2021?

**Regards,**

Shiv Kumar,
Research Scholar,
Department of Human Rights,
School of Legal Studies,
Babasaheb Bhimrao Ambedkar (Central) University,
Vidya Vihar, Raebareli Road, Lucknow - 226025

**Appendix - 5**

**To,** Date: 20.12.2021

The CPIO,
Banaras Hindu University,
Varanasi - 221005, U.P.

**Subject**: Seeking following information under RTI Act, 2005
**Fees:** Postal Order No. 56F 239416 is attached.

**Respected Sir/Madam,**

The applicant seeks following information. Humble request to furnish the same.

1. What kind of social networking sites and apps university is using for imparting online education or intercommunication with staffs?
   a. Googlemeet
   b. Zoom
   c. Webex
   d. Facebook
   e. Youtube
   f. Others ……..
2. Does university have its own software/apps used for online teaching & other purpose free from violation of privacy?
   (a) Yes
   (b) No
3. Is there any policy adopted by the University to protect personal information of students, research scholars, teaching staffs and non-teaching staff?
   (a) Yes
   (b) No
4. What measures is being taken between university and agencies (acting on behalf of university like National Testing agency and others) regarding the processing of personal information of concerned persons (students, teaching staffs, non-teaching staff) to respect, protect the right to privacy?
   (a) Have a MOU between University and agencies not to share personal data with others.
   (b) Delete data after reasonable time period, once purpose is fulfilled.
   (c) Seek consent of concerned persons regarding processing of data like uploading on website
5. Does your university's website www.bhu.ac.in follow any privacy policies?
   a. Yes
   b. No
6. (a) Has any department of university organized privacy awareness program for students in context of social media?
   (b) If yes, how many such programs have been organized from January 2019 to January December 2021?

**Regards,**

Shiv Kumar,
Research Scholar,
Department of Human Rights,
School of Legal Studies,
Babasaheb Bhimrao Ambedkar (Central) University,
Vidya Vihar, Raebareli Road, Lucknow - 226025

## Online RTI Status Form

Note:Fields marked with * are Mandatory.

| | |
|---|---|
| **Enter Registration Number** | BANHU/R/E/21/00722 |
| **Name** | Shiv Kumar |
| **Received Date** | 15/12/2021 |
| **Public Authority** | Banaras Hindu University |
| **Status** | REQUEST DISPOSED OF |
| **Date of action** | 13/01/2022 |
| **Reply :- As desired the available information is given below poitwise:**<br><br>**1. a) Googlemeet**<br>**c) webex**<br><br>**2. No**<br><br>**3. Privacy Policy as available on BHU website:**<br>**new.bhu.ac.in**<br><br>**4. Information not available in the Computer Centre**<br><br>**5. a) Yes**<br><br>**6. Information not available in Computer Centre.** | |
| **CPIO Details :-** | Deepak Kumar (Computer Center)<br>Phone: 9936180508<br>socc[at]bhu[dot]ac[dot]in |
| **First Appellate Authority Details :-** | Sanjay Kumar (Computer Center)<br>Phone: 9451585427<br>coord[at]bhu[dot]ac[dot]in |
| Nodal Officer Details :- | |
| **Telephone Number** | 05422368903 |
| **Email Id** | dradmin1[dot]bhu[at]gmail[dot]com |

**Appendix - 7**

**To,** Date: 20.12.2021

The CPIO,
Rajiv Gandhi National Aviation University (RGNAU))
IGRUA Complex, Fursatganj, Amethi,
Uttar Pradesh PIN 229302

**Subject**: Seeking following information under RTI Act, 2005
**Fees**: Postal Order No. 56F 239418 is attached.

**Respected Sir/Madam,**

The applicant seeks following information. Humble request to furnish the same.

1. What kind of social networking sites and apps university is using for imparting online education or intercommunication with staffs?
   a. Googlemeet
   b. Zoom
   c. Webex
   d. Facebook
   e. Youtube
   f. Others ……..
2. Does university have its own software/apps used for online teaching & other purpose free from violation of privacy?
   (a) Yes
   (b) No
3. Is there any policy adopted by the University to protect personal information of students, research scholars, teaching staffs and non-teaching staff?
   (a) Yes
   (b) No
4. What measures is being taken between university and agencies (acting on behalf of university like National Testing agency and others) regarding the processing of personal information of concerned persons (students, teaching staffs, non-teaching staff) to respect, protect the right to privacy?
   (a) Have a MOU between University and agencies not to share personal data with others.
   (b) Delete data after reasonable time period, once purpose is fulfilled.
   (c) Seek consent of concerned persons regarding processing of data like uploading on website
5. Does your university's website www.rgnau.ac.in follow any privacy policies?
   a. Yes
   b. No
6. (a) Has any department of university organized privacy awareness program for students in context of social media?
   (b) If yes, how many such programs have been organized from January 2019 to January December 2021?

**Regards,**

Shiv Kumar,
Research Scholar,
Department of Human Rights,
School of Legal Studies,
Babasaheb Bhimrao Ambedkar (Central) University,
Vidya Vihar, Raebareli Road, Lucknow - 226025

**Appendix - 8**

**To,** Date: 20.12.2021

The CPIO,
Rani Lakshmi Bai Central Agricultural University
NH-75, Gwalior Road Near Pahuj Dam,
Jhansi, Uttar Pradesh 284003

**Subject**: Seeking following information under RTI Act, 2005
**Fees**: Postal Order No. 56F 239419 is attached.

**Respected Sir/Madam,**

The applicant seeks following information. Humble request to furnish the same.

1. What kind of social networking sites and apps university is using for imparting online education or intercommunication with staffs?
   a. Googlemeet
   b. Zoom
   c. Webex
   d. Facebook
   e. Youtube
   f. Others ……..
2. Does university have its own software/apps used for online teaching & other purpose free from violation of privacy?
   (a) Yes
   (b) No
3. Is there any policy adopted by the University to protect personal information of students, research scholars, teaching staffs and non-teaching staff?
   (a) Yes
   (b) No
4. What measures is being taken between university and agencies (acting on behalf of university like National Testing agency and others) regarding the processing of personal information of concerned persons (students, teaching staffs, non-teaching staff) to respect, protect the right to privacy?
   (a) Have a MOU between University and agencies not to share personal data with others.
   (b) Delete data after reasonable time period, once purpose is fulfilled.
   (c) Seek consent of concerned persons regarding processing of data like uploading on website
5. Does your university's website https://www.rlbcau.ac.in follow any privacy policies?
   a. Yes
   b. No
6. (a) Has any department of university organized privacy awareness program for students in context of social media?
   (b) If yes, how many such programs have been organized from January 2019 to January December 2021?

**Regards,**

Shiv Kumar,
Research Scholar,
Department of Human Rights,
School of Legal Studies,
Babasaheb Bhimrao Ambedkar (Central) University,
Vidya Vihar, Raebareli Road, Lucknow - 226025

**Appendix - 9**

**To,** Date: 20.12.2021

The CPIO,
University of Allahabad,
Old Katara, Prayagraj 211002 - U.P.

**Subject**: Seeking following information under RTI Act, 2005
**Fees**: Postal Order No. 56F 239417 is attached.

**Respected Sir/Madam,**

The applicant seeks following information. Humble request to furnish the same.

1. What kind of social networking sites and apps university is using for imparting online education or intercommunication with staffs?
   a. Googlemeet
   b. Zoom
   c. Webex
   d. Facebook
   e. Youtube
   f. Others ……..
2. Does university have its own software/apps used for online teaching & other purpose free from violation of privacy?
   (a) Yes
   (b) No
3. Is there any policy adopted by the University to protect personal information of students, research scholars, teaching staffs and non-teaching staff?
   (a) Yes
   (b) No
4. What measures is being taken between university and agencies (acting on behalf of university like National Testing agency and others) regarding the processing of personal information of concerned persons (students, teaching staffs, non-teaching staff) to respect, protect the right to privacy?
   (a) Have a MOU between University and agencies not to share personal data with others.
   (b) Delete data after reasonable time period, once purpose is fulfilled.
   (c) Seek consent of concerned persons regarding processing of data like uploading on website
5. Does your university's website www.allduniv.ac.in follow any privacy policies?
   a. Yes
   b. No
6. (a) Has any department of university organized privacy awareness program for students in context of social media?
   (b) If yes, how many such programs have been organized from January 2019 to January December 2021?

**Regards,**

Shiv Kumar,
Research Scholar,
Department of Human Rights,
School of Legal Studies,
Babasaheb Bhimrao Ambedkar (Central) University,
Vidya Vihar, Raebareli Road, Lucknow - 226025