# 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

## ABSTRACT OF 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 (U.P.), INDIA**


**2022**

# ABSTRACT

## 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 the 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- self-regulation.[2]

### 1.1.1 PRIVACY

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

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.[3]

---

[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] Daniel J. Solove, *Understanding Privacy* 1 (Harvard University Press, USA, 2008).

Today, in the backdrop of ubiquitous presence of internet, the right to privacy has come to be understood as 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 multidimensional sphere to the concept of privacy protection.[4]

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 – of 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.[5]

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.[6]

### 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

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

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

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

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.[7]

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[8] of the Universal Declaration of Human Rights (1948) and Article 17[9] of the International Covenant on Civil and Political Rights protect individuals' 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

[7] Prof. Priti Saxena, "Technological Advancements: Enriching or Violating Human Rights?" 20 *JOURNAL OF THE NATIONAL HUMAN RIGHTS COMMISSION, INDIA* 33-34 (December 10, 2021).

[8] 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."

[9] 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."

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.[10]

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. Effective remedy should be provided to the victims.[11]

### 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).[12] 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.[13]

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.

Digital platform, termed 'social media', is the main form of communication, based on networking broadcast, telecast information through social networking sites Facebook,

[10] Molly K. Land and Jay D. Aronson (eds), *New Technologies for Human Rights Law and Practice* 225-226 (Cambridge University Press, New Delhi, 2018).
[11] 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).
[12] S. R. Chauhan and N.S. Chauhan (eds.), *International Dimensions of the Human Rights,* Vol. 2, 691 (Global Vision Publishing House, New Delhi, 2006).
[13] Stephen Currie, *How is the Internet eroding the privacy rights* 25 (Reference Point Press, 2014).

WhatsApp, Twitter, Orkut, My space, Instagram, etc. Social media has a profound impact on the right to privacy and freedom of speech and expression.[14]

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 the access to user data that allows economic user surveillance.[15]

In K. S. Puttiswamy v Union of India[16], 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 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 a times, these websites are hacking in cyberspace which sacrificed personal information of citizens.

[14] Prof. Priti Saxena, "Technological Advancements: Enriching or Violating Human Rights?" 20 *JOURNAL OF THE NATIONAL HUMAN RIGHTS COMMISSION, INDIA* 47 (December 10, 2021).
[15] Supra note 8, at 108.
[16] (2017) 10 SCC 1.

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.[17]

The report[18] 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 a 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.*[19]

Considering the potential threats in the form of communication surveillance, its interception, data theft, unauthorized personal data access, trans-border flow of data etc.

[17] A. W. Haynes, "Online privacy policies: Contracting away control over personal information" *Penn State Law Review* 111, 587 (2007).

[18] 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).

[19] 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).

the UN has affirmed that the same rights that people have offline must also be protected online, including the right to privacy.[20]

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. 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 the totalitarian regimes would use the 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.[21]

In Puttaswamy[22] 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 the 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 on the 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*

[20] 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).
[21] Yuthika Bhargava, "Hacker sees security flaws in Arogya Setu" *Th Hindu,* May 06, 2020.
[22] Justice (Retd.) K.S. Puttaswamy v. Union of India (2017) 10 SCC 1.

*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, Instagram to name a few is not hidden from anybody. The craze with which the 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 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.[23]

Social media is a fast-growing phenomenon in India, as more and more young Indians are getting access to smartphones and 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.[24]

About two-thirds of Indian youth perceive addiction to social media, loss of privacy, fake news and cyberbullying as potential risks of social media.[25]

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 service 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.[26]

---

[23] 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

[24] 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).

[25] 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).

[26] 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).

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).[27]

## 1.3 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 citizens.

(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.

## 1.4 HYPOTHESIS

- Privacy policies of social media are ambiguous, coercive and deceptive.
- Inappropriate legislations are hampering 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

[27] 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).

## 1.5 METHODOLOGY

The proposed research work is analytical, exploratory and empirical in nature. Literature containing provisions of International Instruments of Human Rights, various conventions, national legislations, 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 context of social media. Both primary and secondary data has been used in the research study. Both online communication and personal interaction contact mode have been adopted for gathering information for empirical study. The random sampling method for the data collection has been used.

### 1.5.1 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 universe of the study. Primary data have been collected from the students of these six central universities in Uttar Pradesh.

### 1.5.2 SAMPLE SIZE

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

### 1.5.3 TOOLS AND TECHNIQUES FOR DATA COLLECTION

The data have been collected through the help of both qualitative and quantitative methods. The questionnaire, consisting of 25 different questions has been used to collect primary data from 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, 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 was processed with the help of statistical tools like Statistical Package for Social Science (SPSS) and MS-Excel.

## 1.6 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 may also strengthen the human rights approach to protect, promote and respect the right to privacy of social media users in India.

## 1.7 LIMITATION OF THE STUDY

As privacy is a broad area, hence present study is focussed 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.

## 1.8 SCHEME OF CHAPTERS

**Chapter I: INTRODUCTION**

In order to achieve the objectives of the study, the thesis is divided into seven chapters. Chapter 1 introduces the subject matter. To make an extensive and comprehensive study of the subject, a brief description reflecting on the objective 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, and 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, 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 oe 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.

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.[28]

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.[29] 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

[28]A. W. Haynes, "Online privacy policies: Contracting away control over personal information" *Penn State Law Review* 111, 587 (2007).
[29] Julie J. Beyer, *Privacy: The endangered species of the digital era* 81 (Faculty of Utica College, ProQuest LLC, 2018).

communicate data sharing and collection policies, the ambiguous, vague, and confusing language used undermines the effectiveness and purpose of the privacy policy.[30]

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.[31]

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 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.[32]

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

[30] Julie J. Beyer, *Privacy: The endangered species of the digital era* 22 (Faculty of Utica College, ProQuest LLC, 2018).
[31] Monroe E. Price, Stefaan G. Verhulst, *et.al.* (eds.), *Routledge Handbook of Media Law* 476 (Routledge, New York, 2013).
[32] 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

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.[33]

In 2007, Facebook launched the **Facebook Platform, a set of Application programming interfaces** ("APIs") and tools enabling developers 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,[34] and called for technological measures restricting access to the information that was actually required to run a specific application.

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.

**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 the 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

[33] Ira S. Rubinstein and Nathaniel Good, "Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents" 28 (2) *Berkeley Technology Law Journal* 1394-95 (2013). DOI: https://www.jstor.org/stable/24119897

[34] Ira S. Rubinstein and Nathaniel Good, "Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents" 28 (2) *Berkeley Technology Law Journal* 1395-96 (2013). DOI: https://www.jstor.org/stable/24119897

that leading search engines were tracking their searches and collecting and storing sufficient information.

**Google Street View** has been particularly controversial since the 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.[35]

**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 findings and discussion, 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 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.

One of the most controversial issues in relation to social media websites is their data processing and respect for privacy and personal data.[36] In the modern age data protection is a tool of privacy protection.[37] 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.[38]

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.'

---

[35] JD Christopher T. Anglim (ed.), *Privacy Rights in the Digital Age* 248-249 (Grey House Publishing, USA, 2015).
[36] Dr. Paul Lambert, *A User's Guide to Data Protection* 557 (Bloomsbury Professional Ltd, RH, 2016).
[37] Laura Scaife, *"Handbook of Social Media and the Law* 240 (Informa Law from Routledge, New York, 2015).
[38] Graham Greenleaf, *Asian Data Privacy Laws – Trade and Human Rights Perspective* 5-6 (Oxford University Press, United Kingdom, 2014).

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.[39]

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 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.[40]

Considering the implications of the new technologies, the European Commission concluded that the Directive of 1995 needed to be amended and updated.

On May 25th, 2018, the European Data Protection Regulation came into effect in order to harmonize data privacy laws across Europe.[41] This regulation replaced the Data Protection Directive of 1995.

---

[39] Graham Greenleaf, *Asian Data Privacy Laws – Trade and Human Rights Perspective* 5-6 (Oxford University Press, United Kingdom, 2014).

[40] 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).

[41] General Data Protection Regulation (GDPR). *available at*: https://gdpr-info.eu/ (last visited on May 30, 2022).

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".[42]

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.[43]

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.[44]

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.[45]

The human right 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.

---

[42] 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).

[43] Molly K. Land and Jay D. Aronson (eds), *New Technologies for Human Rights Law and Practice* 225-226 (Cambridge University Press, New Delhi, 2018).

[44] 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).

[45] 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).

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".[46]

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: PRIVACY LAWS AND SOCIAL MEDIA: NATIONAL PERSPECTIVE**

Chapter V is devoted to the legal framework of privacy in the context of social media in Indian perspective.

India does not have any specific data protection mechanism. Statutory protection of privacy is scattered across a number of statutes in India. 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, and is therefore broad enough to include ICCPR Article 17 concerning privacy[47]. It establishes the National Human Rights Commission (NHRC)[48] which has the power to investigate

[46] 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).
[47] Protection of Human Rights Act (India), s. 1(d).
[48] Protection of Human Rights Act (India), s. 3.

alleged violations[49] 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.[50] Its focus has been, and is, on wrongful deaths and other extreme violations.

Section 79 of the 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 society at large from technological innovations.

Interception of any message or class of messages is 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*[51], 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*[52] 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[53]; and (b) ban the use of Zoom applications for official and personal purposes by the public[54]. Blocking of websites under section 69A has also been challenged[55].

[49] Protection of Human Rights Act (India), s. 12(a).
[50] NHRC website www.nhrc.nic.in, See 'Human Rights cases' and 'Suo-Motu Cases'.
[51] *Rahul@Biswajit Sinha v. State of Bengal*, W.P. No. 4483(W) of 2018.
[52] *Facebook Inc. v. The State of West Bengal*, C.R.R. No. 2332 of 2017.
[53] *PIL No. 3 of 2019, Jammu & Kashmir*, High Court (Srinagar Branch).
[54] *Harsh Chugh v. UOI*, WP© No. 10980 of 2020 presently pending before the Delhi High Court.
[55] *Tanul Thakur v. UOI*, Writ Petition No. 13037 of 2017 presently pending before the Delhi High Court.

On June 29, 2020 the Government of India banned 59 apps of Chinese origin[56], 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*[57] 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].

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 the privacy regime. The Government of India appointed a committee of experts for Data protection under the chairmanship of Justice B N Srikrishna which submitted its report[58] in July 2018 along with a draft Data Protection Bill[59]. 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.

New Social Media Rules 2021[60] 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.

---

[56] 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).
[57] *Justice (Retd.) K.S. Puttaswamy v. Union of India* (2017) 10 SCC 1.
[58] B. N. Srikrishna *available at:* https://en.wikipedia.org/wiki/B._N._Srikrishna (last visited on May 30, 2022).
[59] https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf
[60] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

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.

**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 & 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, interpretate 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 analyses and reported along with the findings.

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 and accordingly suggest appropriate measures to be taken in order to protect, and respect the right to privacy of individuals. To serve the aforesaid purpose the researcher has divided the study into two parts: Part A and Part B. 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.

Through data analysis and interpretation, the researcher found that

**Figure 6.14:** Age-wise Participation of Respondents

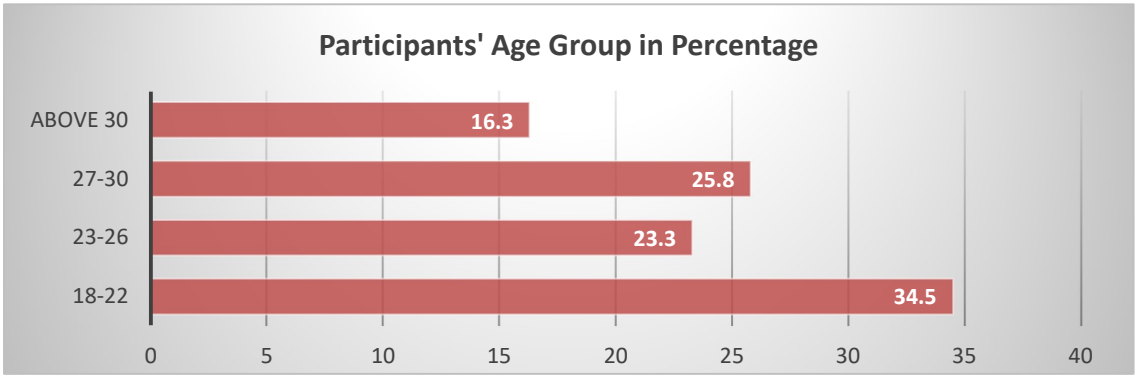



Figure 6.14 shows that maximum participation is from the 18-22 age group i.e. 34.5 % (207 out of 600) while as minimum representation is from the age group above 30 is 16.3 % (98 out of 600). It reflects that those respondents of the youngest age are more addicted to social networking sites and apps.

**Figure 6.16:** Gender-wise participation in survey

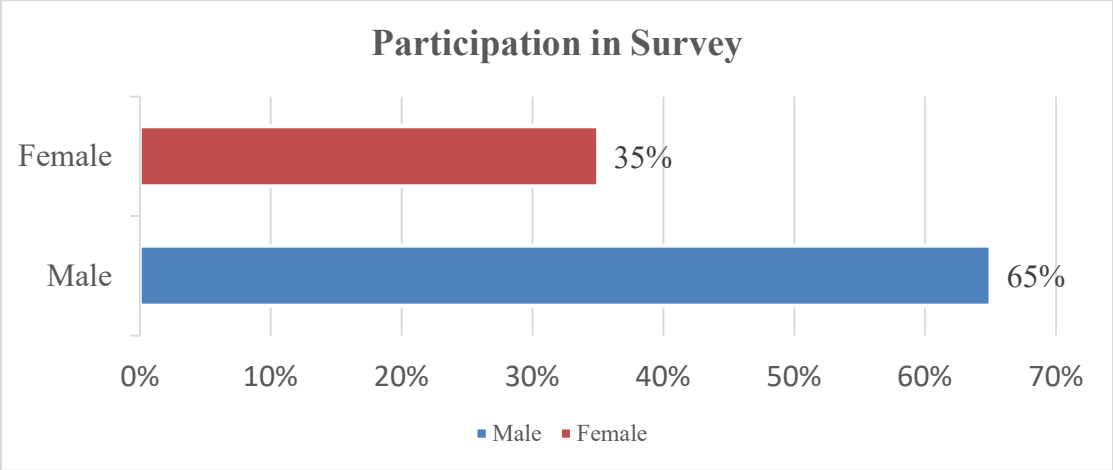



Figure 6.16 depicts that male's participation is 65% (390 out of 600) while as female's participation is 35% (210 out of 600). It reflects that male are dominating in social media's activities in comparison to females.

**Figure 6.18:** Course Pursuing by the Respondents

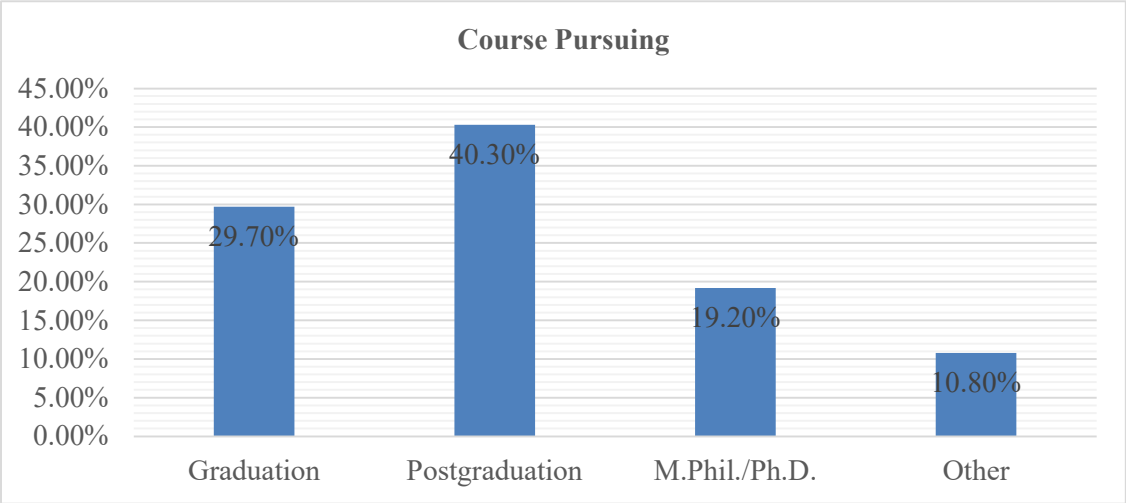



Figure 6.18: shows that the maximum participation course wise is from the students pursuing post-graduation i.e. 40.3%; while minimum participation is from the students pursuing other courses including diploma i.e 10.7 %.

**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%** | **539.5%** |

In response to the question "Which social networking sites (SNSs) /apps do you use?", table 6.22 shows that WhatsApp (16.8%) is the first choice of respondents allowed

by YouTube (15.0%) is the second choice while Facebook (14.1%) and Google (14.1%) are the third choice of respondents.

**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.

In response to the question "When you hear the word privacy, what comes to your mind?" Table 6.30 shows 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 the total responses given (429/1898). Above 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 6.32:** 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.

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".[61] In response to the question "How informational privacy can be best described?" 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.

**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%** |

[61] Alan Westin, *Privacy and Freedom* 1 (IG Publishing, New York, 1967).

a. Dichotomy group tabulated at value 1.

Social Media sites and apps are collecting users' information through overt and covert means. In response to the question "What kind of personal information shared by you is collected by social networking sites /apps?" the researcher found in a survey as Table 6.34 shows that the awareness level of respondents about different types of information collected by SNSs/Apps is very low. Only 9.6% of 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.

**Q. 12. For what purpose social networking sites / apps do use your personal information?**

**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

In response to the question " For what purpose social networking sites / apps do use your personal information?" 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.

**Figure 6.40:** Status of reading privacy policies

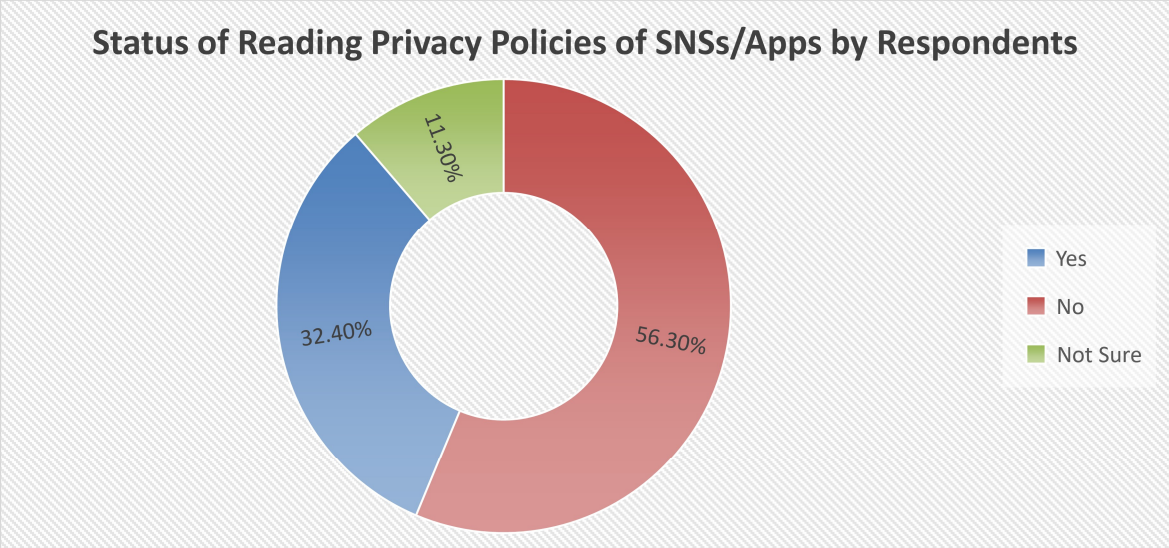



Figure 6.40 shows data received in response to the response "Do you read all the terms and conditions of social networking sites/Apps at the time of registration?" Figure 6.40 show that majority of the respondents 56.3% (335 out of 600) do not read privacy policies/ Terms and Conditions, 32.4 % (193 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. This is alarming situation among respondents that they are not showing concerns towards privacy.

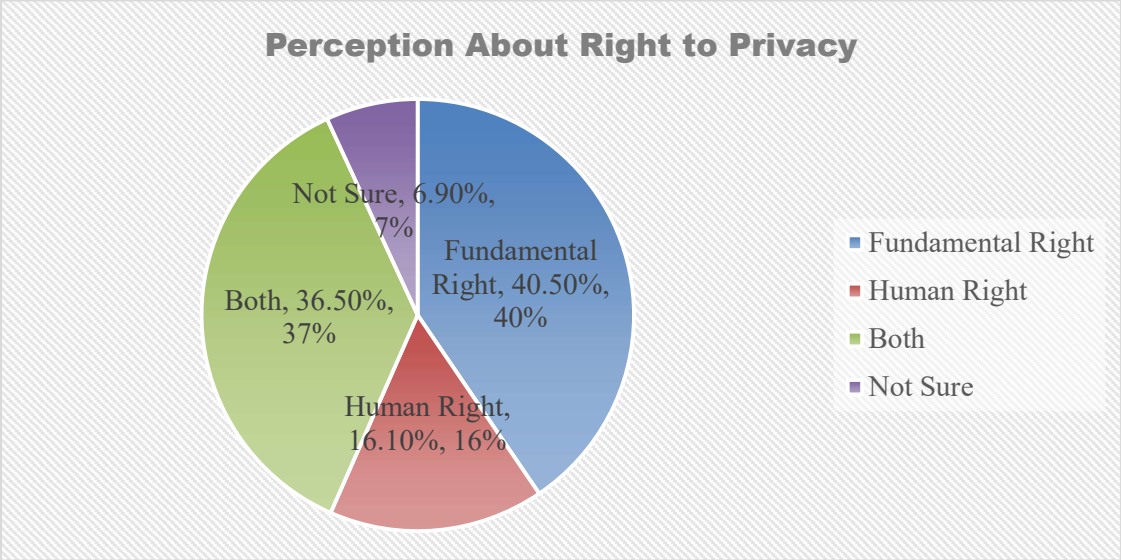
**Table 6.50:** Percent of Cases of $Rights_Data_Subject

| | | 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.

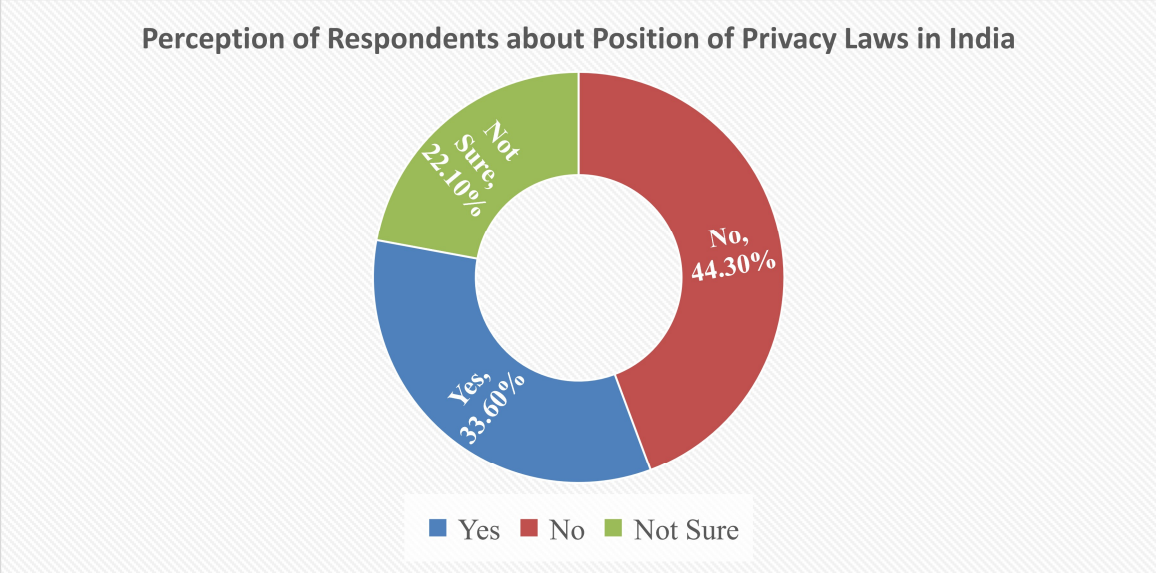
Table 6.50 shows the responses received from the respondents in response to the question "What are the rights of Data Subjects (Social Media Users)?" Table 6.50 shows that only 13.8% respondents are aware about data subjects rights while the remaining respondents are partially aware about data subjects rights. Hence, awareness about data subject rights among respondents is very low.

**Figure 6.52:** Perception about right to privacy




The researcher has tried to know the legal awareness among the respondents about privacy in international law as well as domestic law. Figure 6.52 show that 40.5% of respondents have the perception that the right to privacy is a fundamental right, 16.1% believe that privacy is a basic human right, 36.5% of respondents opined that privacy is a fundamental right, as well aa s 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.

**Figure 6.56:** Privacy Laws in India




In response to the question "Does the Government of India have proper legislation to deal with the protection of privacy of citizens in online social media?" Figure 6.56 shows that 33.6% of respondents have the perception that the Government of India has proper data protection law, while a majority of the respondents 44.3% replied negatively, 22.1% of respondents are not sure about the answer to this question while 0.3% did not respond to this question.

**Table 6.58:** Percent of cases of $Data_Protection_Principles[a]

| | | 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 the responses received from respondents in response to the question "What do you expect from social networking sites and apps while processing your personal

data?". Table 6.58 shows that 374 respondents expect that the processing of personal data must be fair and lawful, this total represents 24.9% of the total response 317 respondents opined that personal data must be processed for limited purposes, this is 21.1% of the total response. 295 respondents say about data quality i.e. data must be adequate, relevant and not excessive which represents 19.7% of the total response. 297 respondents talk about data security (personal data must be secure) which is 19.8% of the total response. 201 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 which represents 13.4% of the total response. Hence, it shows that awareness of data protection principles among respondents is not satisfactory.

**Figure: 6.62:** Privacy Awareness Programme

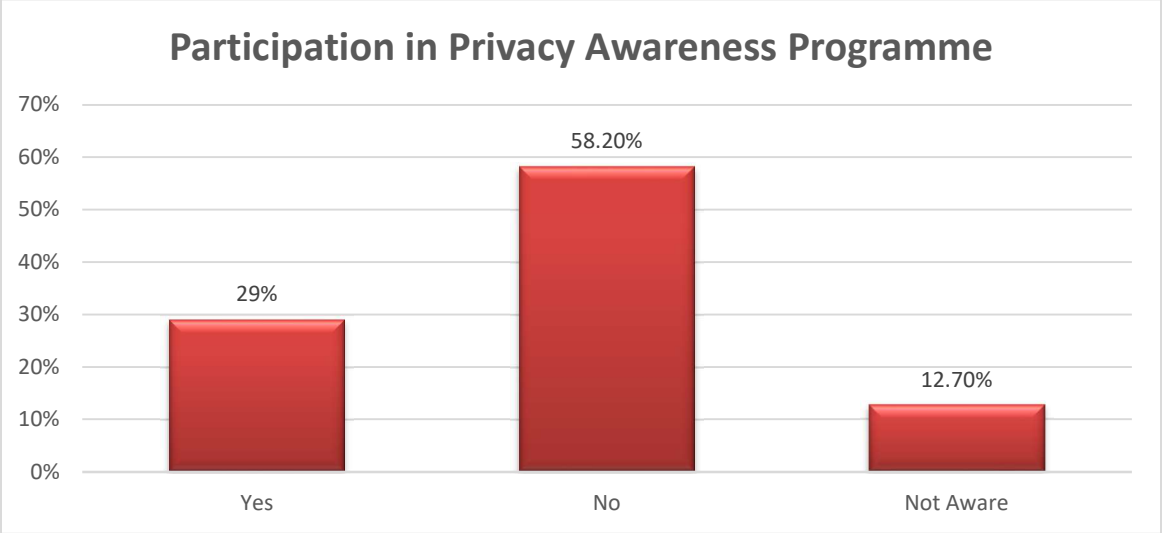



Figure 6.62 shows the data received in response to the question "Have you ever participated in any program organized by your university to spread awareness about privacy/cyber issues in online social media platforms?".

Figure 6.62 shows that 29% of respondents participated in a privacy/cyber issues awareness programme organized by the concerned university. 58.2% of respondents did not participate in any privacy/cyber issues awareness programmes, 12.7% of respondents are not aware of such programmes while as 1.8% did not respond to this question.

Apart from information received from 600 respondents from six central universities in Uttar Pradesh, the researcher also asked authorities' privacy. Only two universities Aligarh Muslim University (Aligarh) and Banaras Hindu University (Varanasi) responded to the queries of the researcher while 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.

**Figure 6.64:** RTI response from universities

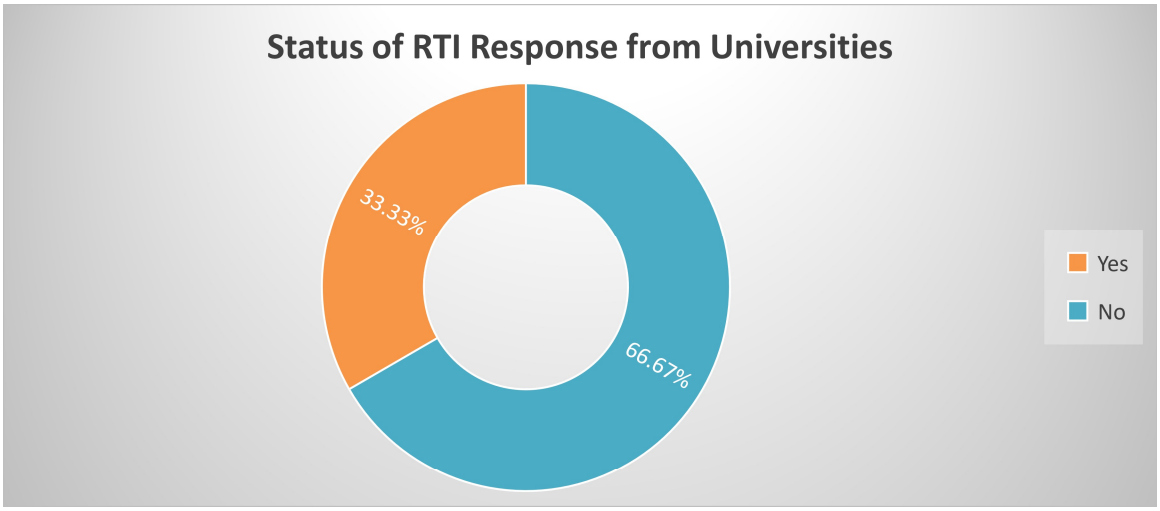



Figure 6.64 shows that only 33.33% of universities responded to the queries of the researcher while 66.67% of universities did not respond to the queries.

- 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.

- 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 to 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**

The concluding chapter presents the research study with reference to the theoretical and empirical 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 before sharing it with social networking sites/Apps.

## 1.9 CONCLUSION

Privacy is an issue of profound importance around the world. 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.

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. Privacy policies of social networking sites seem problematic being coercive, deceptive and ambiguous.

Lack of awareness about privacy issues among citizens in online social media, Self-regulation mode, capitalism model, deceptive privacy policies of powerful social networking sites (SNS) have enabled social media to intrude sacred precincts of the domestic and private life of a citizen.

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. The DPD was enacted in 1995, prior to social media, cloud computing, mass data storage, data mining, electronic profiling/Web 2.0 and the threats to the data security surrounding personal data. This was even before the spotlight centered on abuse issues. Data protection needs to evolve to deal with, or at least more explicitly deal with, these issues. This is partly the reason for the new EU GDPR.

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".[62]

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.

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. Inappropriate legislations are hampering the protection of the privacy rights of social media users.

The research shows that students do not concern about their privacy. The researcher found that awareness regarding legal provisions and privacy policies of social media among the students of central universities in Uttar Pradesh is not adequate.

The researcher found that privacy concerns of central universities in Uttar Pradesh are not satisfactory. Most of the universities are mostly dependent on social networking sites/apps for imparting education. They don't have their own software. The survey shows

[62] 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).

that programmes organized by universities to make students aware of privacy/cyber-related issues is negligible.

## 1.10 SUGGESTIONS

1. There are large gaps in our knowledge, research and understanding of developing issues in social media platforms. More research is needed to appraise ourselves of all potential solutions and policy decisions as well as assist 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 the rights of vulnerable 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 ensures 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 from 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 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 the digital age we need to know the value of the personal information that we share online and other aspects like who is gathering data about us, how that data is used by whom, and 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 the 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 on social media platforms.

### 1.10.1 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.

### 1.10.2 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 with easy mechanisms to access 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.

### 1.10.3 RECOMMENDATIONS SPECIFIC TO HIGHER EDUCATIONAL INSTITUTIONS

**a.** Higher Educational Institutions must adopt mechanisms to respect and protect the right to privacy of students, and 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.

### 1.10.4 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.

## 1.11 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 explore 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.