LEGAL LIABILITY FOR PRIVACY VIOLATIONS ON SOCIAL MEDIA: A CRITICAL ANALYSIS OF FACEBOOK.

Dissertation submitted in part fulfillment for the requirement of the Degree of LL.M

SUBMITTED BY
SIBANDA THANDOLWENKOSI
ADMISSION NO'' 23GSOL2060001
ENROLLMENT NO'' 23102060001

UNDER THE SUPERVISION
OF
DR. PALLAVI GUPTA

GALGOTIAS UNIVERSITY

(Established under Galgotias University Uttar Pradesh Act No. 14 of 2011)

GALGOTIAS UNIVERSITY, SCHOOL OF LAW
(2023-2024)

DECLARATION.

I, SIBANDA THANDOLWENKOSI hereby declare that the dissertation titled "Legal liability for privacy violations on social media: A critical analysis of Facebook." is submitted by me in partial fulfillment of the requirement for the award of the LL.M(Masters in Law) Degree. This is based on original research undertaken by me under the supervision of Dr. Pallavi Gupta, School of Law, Galgotias University, Uttar Pradesh and has not been submitted in partiality or fully in any University for any degree or diploma.

SIBANDA THANDOLWENKOSI
23GSOL2060001
23102060001
SCHOOL OF LAW
GALGOTIAS UNIVERSITY
GREATER NOIDA, UP

SUPERVISOR'S SIGNATURE

This is to certify that the dissertation titled "Legal liability for privacy violations on social media: A critical analysis of Facebook." has been prepared by Sibanda Thandolwenkosi pursuing LL.M from School of Law, Galgotias University under my supervision and guidance. I recommend it for evaluation.

Place

Date

ACKNOWLEDGMENT

I would like to express my heartfelt gratitude to the following amazing individuals who saw me throughout the writing of this dissertation journey without any complains.

First and foremost, I would like to thank my amazing and esteemed mentor Dr. Pallavi Gupta (Assistant Professor, School of Law, Galgotias University) for her unwavering support, encouragement and incredible patience throughout this journey. Her guidance and expertise ave been invaluable in shaping my research and helping me navigate the challenges along the way. I'm truly grateful for her dedication. Thank you ma'am.

I would also like to thank Dr. Shivangi Sharma (Program Chair, LL.M, Associate Professor, SOL), Dr. Vinayak Pandey, (Division Chair, LL.M, Assistant Professor, SOL) and my other faculty members of the school of law for their valuable insights and constructive criticism throughout the entire journey of my dissertation. Their guidance and suggestions helped me so much and for that I am grateful.

I thank all my friends and family for rendering their support, kindness, encouragement and understanding during this time.

Above all, I'm grateful to the school of law of Galgotias University for providing me with valuable materials and pleasant atmosphere especially the library to do my research for this dissertation.

SIBANDA
THANDOLWENKOSI

LIST OF ABBREVIATIONS

- ATM. Automated Teller Machine
- AV. Anti-virus
- CEO. Chief Executive Officer
- DNS. Domain Name System
- ECC. European Cybercrime Centre
- EPIC. Electronic Privacy Information Centre
- FB. Facebook
- FTC. Federal Trade Commission
- GDPR. General Data Protection Regulation
- IAP. Internet Access Provider
- ICS. Industrial Control System
- IG. Instagram
- IP. Internet Protocol
- ISP. Internet Service Provider
- IT Information Technology
- IWF. Internet Watch Foundation
- LEA. Law Enforcement Agency
- MOTO. Mail Order/ Telephone Order
- NAT. Network Address Translation
- NISb. Network and Information System
- OTP. One-time password
- PIN. Personal Identification Number
- RAT. Remote Access Trojan
- UCC. United Cyber Caliphate
- URL. Uniform Resource Locator
- VoIP. Voice-over-Internet Protocol
- VPN. Virtual Private Network

- WWW. World Wide Web

LIST OF CASES

- EPIC v. FTC
- FTC v. Facebook
- FTC v. Facebook
- Gabriel Darley Melvin v. Dorothy Davenport Reid
- Google Spain SL, Google Inc. v. AEPD, Mario Costeja Gonzalez.
- Karmanya Singh Sareen v.Union of India
- K.S. Puttaswamy v. Union of India.
- R. Rajagopal v. State of Tamil Nadu
- Sri Vasunathan v. Registrar General
- Smith v. Facebook.
- V. v. High Court of Karnataka

TABLE OF CONTENTS

Chapter 3- Facebook as a Social Media Platform

- Privacy related issues with Facebook
- Legal privacy cases against Facebook
- Case laws
- Smith v. Facebook
- Karmanya Singh Sareen v. UOI

Chapter 4: Legal Liability

- Understanding the fault
- Facebook's fault
- User's fault
- Third party's fault
- Preventive Measures
- Conclusion

Chapter 5: Privacy and Data Protection

- Modern day definition of Privacy
- The importance of Data Privacy
- Principles of Data Privacy
- Data Protection and privacy
- Data Protection
- Principles of Data Protection
- Privacy as a Right.
- Right to be Forgotten
- Privacy and Right to Free Speech
- Legislative Framework
- GDPR
- IT Act
- Personal Data Protection Bill
- Right to Information Act

Chapter 6: Conclusion and Suggestions

- Future recommendations
- Contribution to the Field

LEGAL LIABILITY FOR PRIVACY VIOLATIONS ON SOCIAL MEDIA: A CRITICAL ANALYSIS ON FACEBOOK.

CHAPTER 1- INTRODUCTION.

"Even though society as a whole is increasing the amount of personal information available to the public, there is still an expectation of privacy. People believe, sometimes falsely, that they can control the personal information they hold out to the public by determining who can access the information and how the information will be used. It is extremely challenging to define a fluid concept like privacy because it touches almost every aspect of a person and society to one degree or another."[1]

- Daniel J. Solove

In a world like today where social media has become the norm and the order of the day, it is important to take a step back and evaluate how our personal information is being handled on these platforms. Privacy and Data protection in social media is of utmost importance and user confidentiality is becoming even more important. The above statement by Daniel J. Solove touches a significant issue in today's digital age. Indeed, while society is sharing more personal information than ever before, individuals still maintain an expectation of privacy. This expectation, however, can sometimes be at odds with the reality of information sharing and data processing technologies.

Information shared online can be negatively used in several ways, and it's important to be aware of these risks to protect oneself. Some of the impacts include privacy risks, damage to one's reputation, hacking, identity theft, cybercrime even more targeted advertising. It is important to exercise caution when sharing information online and to use privacy settings.

Social media refers to a variety of technologies that facilitate the sharing of ideas

[1] Solove, Daniel J., Understanding Privacy. Daniel J. Solove, UNDERSTANDING PRIVACY, Harvard University Press, May 2008, GWU Legal Studies Research Paper No. 420, GWU Law School Public Law Research Paper No. 420.

and information among their users. It can be defined as online platforms and websites that allow people to create, share content, connect with others and engage in virtual communities. In this digital era, social media has become important as a way in which people interact and stay connected in a digital world.

Social media has become a major concern for cyber security community due to its ubiquitous nature targeting all without discriminating. Be it youngsters or the elderly, or an entire nation's population, social media is available to all without much control on content and practices on its vicinity.

Social networks like Instagram, X, WhatsApp, Tiktok, Tinder, YouTube among other others have become an integral part of our day to day lives. From personal information such as text, photos, videos, music to academic related information, its all being shared everyday on these platforms with so little privacy being preserved. Information is easily found online nowadays, privacy has become so foreign and unprotected.

Facebook as a social media platform has been constantly facing backlash due to privacy concerns. On several occasions, user's privacy has been violated which has led to questions about the legal liability of these actions. Facebook has been accused of violating its users' privacy rights by enabling third parties to access their personal information without their permission. The corporation has faced several inquiries and lawsuits from agencies and consumers all around the world. In 2019, Facebook agreed to settle the accusations by paying a record-breaking $5 billion fine to the Federal Trade Commission, as well as submitting to new limitations and a restructured corporate structure.

Social media as a concept has made the lines of privacy so hazy so much more that people cannot differentiate between truth and falsity, information and misinformation. Due to the nature of social media, being the most enormous and influential market place today, it is becoming harder to regulate it as time passes. This is why the biggest challenge faced by Governments and Law Enforcement Agencies today is to regulate and maintain social media.

Since so much information is being shared on social media platforms it is important to know how the said information is being used. Privacy and data issues

have become a concern to many if not all of us over the years when it comes to social media. Personal data held by social media platforms is also vulnerable to being accessed and misused by third parties, including law enforcement agencies.[2]

Privacy itself is an old-age concept which can be difficult to define. The definition of privacy depends one's standpoint. It could be defined as one's wish to remain unidentified in the public realm, yet it could also be defined as ones' right to be left alone as according to U.S. Justice Louis Brandeis[3] Privacy within its ambit is closely affiliated with basic human rights such as human dignity, liberty, freedom, therefore a fundamental right. The definition of privacy is therefore a controversial issue that is difficult to fully comprehend.

Privacy has frequently been defined as the state of being free from unwanted or unwarranted intrusion or disturbance in one's private life or affairs; the ability to be left alone in one's space without anyone's interference. Its freedom from negative press, public scrutiny, covert monitoring, or unauthorized exposure of personal information by a company, government, or individual. Because so much information about us is available online, it's possible that personal privacy will become obsolete.

When it comes to the legality of right o privacy, it is important for one to recognized and comprehend the difference between privacy and that which is legally protected. These two concept might sound similar and same but are in fact different depending on ones understanding of the two. Privacy for instance is my right to control the usage of my personally identifying information and protection would be how social media platforms protect and secure my information from external and third party violation.

While data and privacy protection in social media are governed by laws and regulations, the privacy laws in India and globally are comparatively weak. When it comes to social media and privacy regulation, the Indian legislature and courts have fallen well short of expectations in terms of the drafting of laws. Strict regulations for the protection of sensitive personal data have been developed and are being followed by financial intermediaries and service providers. Owing to privacy being

---

[2] Social Media Privacy – EPIC – Electronic Privacy Information Center

[3] Warren, Samuel; Brandeis, Louis (December 15, 1890). "The Right to Privacy". Harvard Law Review. IV (5): 193–220. Retrieved 4 June 2021 – via Internet Archive.

recognized as a human right, the scope of privacy now includes data security. Data Protection Bill, 2020 was introduced in light of this.

The Constitution of India under article 21 has tried to incorporate the right to privacy in the fundamental right to life and personal liberty. According to Art 21 of the Indian Constitution, *"No person shall be deprived of his life or personal liberty except according to procedure established by law."*[4] Even though the right to privacy is nowhere mentioned either in this article or article 19(1), the courts have managed to pronounce it as a constitutional right by virtue of articles 21 and 19. This was pronounced in the landmark judgment of K.S. Puttaswamy v. Union of India (2017) where the Supreme Court recognized the right to privacy as a fundamental right protected under Article 21. The court held that privacy is an essential aspect of personal liberty and dignity and is intrinsic to the entire constitutional scheme though subject to certain restrictions.[5]

The Information Technology Act, regulates penalties for data theft and electronic data privacy. The IT Act 2000 includes provisions to protect personal data and privacy as it also defines various offenses related to data privacy and protects sensitive data stored by social media and other electronic intermediaries. One such specific provision is by way of Section 66E of the IT Act 2000 which deals with the violation of privacy and punishes the act of knowingly sending pictures of a person's private parts without their consent.[6]

In the United States, the important laws pertaining to social media privacy are the Communications Decency Act (CDA) and the Children's Online Privacy Protection Act (COPPA)[7]. Currently, privacy in social media is not specifically regulated by US laws , but there have been various attempts made to strike a balance between data collection and users' right to privacy.

The right to privacy is also part and parcel of the 1950 European Convention on Human Rights, which states, *"Everyone has the right to respect for his private and*

[4] Article 21: Protection of life and personal liberty - Constitution of India

[5] Justice K.S.Puttaswamy(Retd) vs Union Of India, AIR 2018 SC (SUPP) 1841, 2019 (1) SCC 1, (2018) 12 SCALE 1, (2018) 4 CURCC 1, (2018) 255 DLT 1, 2018 (4) KCCR SN 331 (SC), AIRONLINE 2018 SC 237 via Justice K.S.Puttaswamy(Retd) vs Union Of India on 26 September, 2018 (indiankanoon.org)

[6] India Code: Information Technology Act, 2000

[7] ACLU v. Gonzales - Challenge to Child Online Protection Act | American Civil Liberties Union

family life, his home and his correspondence."[8] It was on this basis that the EU enacted the General Data Protection Regulation (GDPR)[9]to data privacy and security standards. The GDPR intends to offer people more control regarding the data they give to entities, including the ability to request to erasure.

There are so many questions surrounding this concept such what is protected, and not protected, how is shared data being used, who has access to such information? All these questions have not been clearly answered in terms of data and privacy in social media.

[8] Right to respect for private and family life - The European Convention on Human Rights (coe.int)
[9] What is GDPR, the EU's new data protection law? - GDPR.eu

STATEMENT OF THE PROBLEM

As of today, thousands of people dominate prominent social media platforms such as Instagram, Facebook, Snapchat, TikTok, YouTube, Twitter, LinkedIn, and dating websites. The privacy dangers of social platforms are aggravated by substrate centralization that enables dominant social media corporations to purchase competitors, exert monopolistic power, and severely impede the growth of privacy-protective alternatives. Personal data stored on various social networking platforms is also subject to unauthorized third-party access and misuse, including by judicial agencies.

The legal issue arising out of the use of mobile applications and social media per se is privacy. Most social media platforms collect personal information about its users and use it without their express consent. While the use of the users information is governed by the privacy policy of the app, most users are unaware of the implications of the said policies. When they consent to Terms and Conditions, they do not even read the said T&C's nor do they understand what exactly they are consenting to. I'm not sure this is ignorance or naivety.

Social media and networks are one of the largest frontiers today for lawyers, academics, lawmakers, politicians and entrepreneurs. This is because of the new opportunities presented by the rapid growth of technology and rise of digital world that allows people to connect and communicate in new ways. While this all good and rosy, we tend to ignore the risks and dangers posed by this concept. Ignorance is not being naive because at least we are all aware of the risk but just choose to turn a blind eye to it. And this is because one way or the other, be it lawyers, entrepreneurs or innovators, they are all benefiting from this alluring world of social media.

The massive storage of personal data that social media platforms collect and retain is vulnerable to hacking and data breaches, especially if platforms fail to institute critical security measures and access restrictions.[10]If adequate security measures and access controls are not implemented, the data can become susceptible to

[10] Social Media Privacy – EPIC – Electronic Privacy Information Center

unauthorized access through hacking, phishing, or other forms of cyberattacks. The data at risk ranges from personally identifying information such as name, date of birth, email address, location, personal images, sexual orientation, health information and more. The consequences of exposing this information can be severe and detrimental to an individual's life and a clear violation of basic human rights

The integration of humanity and social media continues to grow. According to Statista, a German platform that specializes in data gathering and visualization there are 5.35 billion internet users worldwide, which amounted to 66.2 percent of the global population and out of this total, 5.04 billion, or 62.3 percent of the world's population, were social media users.[11] And this was in January 2024, you can imagine how many active social media users there are as of today.

While all the talks of social media violating its user privacy goes around, it is important to note that most times users contribute to the said violation and then have a misguided privacy expectation directed towards social media companies. What users fail to understand is that in in the social media setting, it is rarely the social media firm that violates privacy. And this brings us to the question of the legal liability on the said actions. Who shall be responsible for violations committed by users' against user's or by the corporation against user's or even user's against the corporation's privacy policies.

The netizen inadequacy knowledge about the dangers of engaging in social media and amplifying cybercrimes committed in the virtual community has become a concern in his digital era. The constant increase in social media usage raises concerns about not only privacy and data protection but also intellectual property disputes. It is important to take a step back and analyse if users can truly comprehend their consent actions.

[11] Internet and social media users in the world 2024 | Statista

LITERATURE REVIEW

Various authors and academia have done tremendous research on either social media usage or privacy issues in social media world. There is a lot of literature that can be found in books, journal articles, court proceedings, research papers, or even new articles pertaining to privacy issues in social media. One such book is the Facets of Media Law by Madhavi Goradia Divan that examines various aspects of media law including the right to privacy and social media.

Westin, who is regarded as the father of the modern concept of privacy defined it as the claim of an individual or a group or organization to determine, when, how and to what extent can information about them be communicated to others. [12]

The private information has nowadays become of so much value than is realized by the owners of the data to the extent that they trade it for mere peanuts.

Feldman was of the view that, "The job of protecting privacy and security online becomes more complex. Consumers, in order to avail of full benefits of online transactions, such as the ease and speed of processing an online order, trade off by allowing companies access and use of private data.". [13]

According to this literature review, the media has rendered it feasible to bring someone's private affairs into the public eye, exposing him to a likelihood of violation of his privacy. This is something that was far fetched prior to the media era.

Statistics and studies show that there have been so many cases relating to social media violating its user's privacy and data. Findings have also shown that most crimes are committed against users on these social media platforms due to lack of privacy protection. Information submitted or entered online, and data collected has many times been used for targeted advertising. Social media companies like Facebook collect vast quantities of personal data to micro target advertisements to users which violates user's privacy, the flow of information, and the psychological health of social media users.

[12] Westin, A. (1967). Privacy and freedom. New York: Athenaeum
[13] Feldman, A.,2000. Protecting Your Financial Privacy. Money, 29(6),pp. 161 -164

OBJECTIVES

A better knowledge of how people view privacy issues can provide useful insights for both professionals and scholars worldwide. While social media platforms such as Facebook have standards in place to protect privacy, there is still worry about legal culpability for infractions committed on the network. Although there have been several research on online privacy in general, there is a paucity of studies that explain the unique nature of information privacy and user rights, particularly when it comes to the usage of social networking sites. It is also important to create awareness about the importance of understanding privacy policies in social media so that the users might have clear knowledge of what they are consenting to on these platforms.

This paper objectively aims to:

- Analyse the legal liability for privacy violation on Facebook.
- Analyse social media compliance with legal frameworks.
- Look at the laws and regulations put in place to safeguard and protect users' privacy and data as well as to see how far the government has gone to implement these.
- Delve privacy risks associated with social media usage.
- Understanding user rights and educating users about privacy settings.

1.2 HYPOTHESIS

Social media platforms like Facebook's current privacy and data protection measures are insufficient to ensure users' privacy, which causes risks of personal information misuse and privacy breaches. The legal liability of violations committed on Facebook lies with both the corporation and the users alike.

RESEARCH QUESTIONS

- Who is liable for privacy violations committed on Facebook.
- Do users comprehend the consequences of their consent when accepting the T&C's,
- Why are there concerns surrounding privacy in social media.
- Why it is important to understand social media privacy policies before using it.
- Why it is important to introduce and implement laws and regulations to protect data and privacy in social media platforms.
- What does social media do to protect user's privacy and data.
- What remedies are available to those whose privacy has been violated in social media or by social media platforms.
- How secure is user information stored on these platforms.

1.3 RESEARCH METHODOLOGY

For this paper, various research methodologies were used to gather information such as literature review, case studies, observations and experiments. I did a thorough perusal and research on studies including books, academic papers or published statistics pertaining to privacy and data protection in social media.

All in all, the research methodology used was a doctrinal method of research wherein primary and secondary sources of research like books, articles, bare acts among others were used.

1.4 TENTATIVE CHAPTERISATION.

1.4.1 This dissertation has been divided into 6 (six) Chapters:

- CHAPTER I : Introduction
- CHAPTER II : Social Media - Concepts and Contours
- CHAPTER III : Facebook As A Social Media Platform
- CHAPTER IV : Privacy and Data Protection Issues
- CHAPTER V : Legal Liability.
- CHAPTER VI : Conclusion and Suggestions.

1.4.2 Summary of Chapters

Chapter I is an introductory chapter

Chapter II introduces social media, its historical background, terms and conditions. This chapters also delves into social media's privacy policy and analyses the impacts of its usage.

Chapter III deals with Facebook as a social media platform and analyses the legal case law regarding to privacy violations.

Chapter IV deals with legal liability of privacy violations committed on Facebook.

Chapter V deals with privacy with regards to privacy and data protection in social media. The chapter also analyses privacy issues arising out use of social media and legal framework surrounding social media at large and media law in passing. It analyses the statutory provisions governing social media privacy disputes.

Chapter VI is the closing chapter. It includes conclusion and suggestions.

1.5 SCOPE OF STUDY AND LIMITATIONS.

1.5.1 The scope of this study is focused on the legal liability of privacy violations on Facebook and social media at large. It studies the privacy policies of social media platforms while highlighting the privacy issues arising out of its usage. The study further looks at the legal frameworks or laws governing privacy in social

media and critics their effectiveness in protecting users right to privacy.

1.5.2 This paper is limited to privacy issues arising out of Facebook usage. Some concerns about the use of social media like cyber crimes including but not limited to scamming are not thoroughly discussed here. They might have been at one point briefly discussed but the focus is not on them.

CHAPTER 2

CHAPTER 2- UNDERSTANDING SOCIAL MEDIA USAGE.

INTRODUCTION TO SOCIAL MEDIA.

The technological advancement has made it extremely easy to share information and connect with anyone and everything across the globe whenever and however one wishes. The desire and need for information technology has amplified greatly owing to the fact that social media sites can be easily accessed as long as one has internet access. The increase in growth, popularity and usage of social media has however led to gross emergence of cyber crimes and criminals.

As of early 2024, Zimbabwe was home to 2.05 million active social media users, which equates to 12.2 percent of the total population of 16.32 million people at the start of the year, with a median age of 18.5 years.[14] Statistic records from researches have shown large presence of users on these platforms owing to easy access to technology. The use of social media has never been an issue before as it is now and this because people are sharing their information which might not be as safe as they would like to think.

While social media began as a medium for interaction between relatives and close companions, it eventually came to be used for a variety of activities. Today, social media is being criticized for spreading hate speech and misinformation while also being praised for aiding in the development of communities. It has become an increasingly important part of many companies' marketing campaigns with Facebook dominating the social media landscape.

Social media is a way for people to connect and share things online. It is all about connecting with people online and sharing information like photos, videos, music and thoughts. It can be termed as a virtual community where people chat with friends, follow each other, discover their interest and keep updated on news. Wherein Virtual community, can be described as an ensemble of people who communicate words and ideas via digital networks, whether or not they meet in

[14] Digital 2024: Zimbabwe — DataReportal – Global Digital Insights

person. Its generally a great way to stay connected, entertained and discover new things.

Users typically access social media services via web-based desktop software or services that provide social media capabilities for mobile devices. Users engage with various online services to build highly dynamic platforms in which individuals, groups, and organizations communicate, co-create, talk, contribute, document experiences, discover and explore things, promote themselves, form connections, and promote ideas.

While the use of social media is still mostly voluntary, businesses have been pressuring users to upgrade to paid subscriptions in order to lessen their reliance on advertising revenue. One such example is Meta Verified which attracts users with a blue verification mark and proactive account protection. Users can also enhance their social media profiles on X (previously Twitter), Snapchat, and Reddit for a monthly fee.

Social media has become a phrase people use a lot nowadays to describe what they post on sites and apps like Facebook, Instagram, Snapchat, Tinder and others. It could therefore be of inference that social media are web-based sites that allow people to interact with each other. The term social media has however became so vague that it can basically describe nearly any website on the World Wide Web today.

Social media is a type of mass media communication on the Internet wherein users share ideas, knowledge, private messages, and other content. Although social networking and social media are similar concepts, it is vital to distinguish between the two. Social networking is typically defined as people creating communities among themselves, but social media is more about leveraging social networking sites and associated platforms to generate an audience.

To avoid this confusion, the definition of social media must be broken into two words; social and media. 'social' refers to interacting with other people by sharing information with them and receiving information from them. And 'media' would be defined as a communication tool, such as the internet (conventional kinds of media include TV, radio, and newspapers). Thus, social media are online communication

platforms that allow people to interact with one another by sharing and consuming content.

So while the definition of social media can be confusing, fact is we all can spot it as it comes. We all have some kind of basic understanding as to what social media entails. Social media is regarded as the numerous types of communication over the internet used by people to construct networks, groups, and communities to exchange information, ideas, messages, and other material, like videos.

From the above definition it could be inferred that social media relies on user-generated content and requires online communication, hence its history cannot predate the internet's widespread adoption. This explains why conventional blogs and websites are not included in the social media landscape. Only certain individuals have the right to publish on these platforms, and the content that can be submitted is highly regulated.

Today, there are so many social media platforms that enable users to connect, be entertained and share content worldwide. Social media is a way to transmit, or share information with a broad audience.

Social networks, such as Twitter and Facebook, enable people to connect with family, friends, firms, and strangers. Users can follow each other online and share images, life updates, random ideas, and other content. Businesses can leverage social media for marketing and customer service.

Media-sharing networks these are networks for sharing media, like YouTube, Instagram, Snapchat, TikTok, and others, that users use to exchange images, videos, and other kinds of content. Social media influencers, sometimes known as famous users, use media-sharing platforms to influence their audiences' shopping habits, lifestyles, and other elements. Businesses can develop partnerships with influencers to market their products and services to specific audiences.

Discussion forums- these are online platform that enables people to engage in ongoing conversations and share information about a particular topic or theme. These forums are often created on community engagement platforms designed for business use. Platforms such as Reddit discuss a large number of topics, businesses can use discussion forums to gain research insights into new potential markets.

Companies can create advertisements, answer consumer questions, and provide customer service by responding to compliments and complaints. They can also crowd-source ideas for products and launches. Forums help companies connect with customers, gather feedback, and establish a sense of community, and they are also an opportunity for users to connect with like-minded people and participate in a shared experience.[15]

Consumer reviews- these are review platforms where customers can leave feedback about products or services for others to read. These platforms allow users to leave feedback about products or services and help others make informed decisions. They also play a significant role in a company's reputation and can influence marketing efforts. Facebook, Yelp, TripAdvisor, G2, Review io, Gass Door are some examples of consumer review platforms.[16]

[15] A Deep Dive into Discussion Forums - benefits, best practices, and what to look for in a platform
[16] The 12 Most Credible Review Platforms for Customer Feedback (10to8.com)

Salient Features of Social Media

Social media is one of the popular ways of modern communication which offer various functions for communicating and sharing information among the public. Social media platforms have salient factors that can be explained as:

- User Profile: Users make personal profiles that depict their point of view, interests, personal information, and activities. They share and post the content and follow other profiles vis-a-vis. Several platforms provide services after users make their accounts on their platforms. Some profiles are verified to fully utilize the platforms in consideration of a monthly fee.
- Connectivity: Users can connect with friends, family, and like-minded individuals, expanding their social networks beyond geographical boundaries. This is mostly done online, over the internet. Most social media users on platforms like Facebook, Instagram, X, Messenger, WhatsApp to mention just a few, use these platforms to keep in touch with their loved and friends. This is helpful in cases where people are worlds apart from each other. Social media helps with staying
  in touch.
- Content Sharing: Users share content like photos, videos in the form of reels, text-based posts, stories, music among others to their followers wherein content with reference to social media includes any works or invention created by individuals or companies for social networks. The content shared by users easily becomes viral, reaching a wide range of audience due to the ease of sharing and engagement. The content shared is usually diverse which promotes cultural diversity among users.
- Interactivity: There are features such as likes, comments, and shares that encourage users to engage and interact with others. Users can interact directly with each other and with brands to promote their works and that of others too.
- Customization: Users can customize their profiles and accounts through privacy settings, profile management, and personalized feeds. The customization feature give users the flexibility to configure their user settings,

customize their profiles to their liking, manage the information they see in their news feeds and even give feedback on what they do or don't want to see especially advertisements.

- Notifications: This feature keeps users informed about activities related to their profile, friends, content shared and their interests. Users have to enable Alerts and Notifications on their accounts to fully utilize this feature.
- Mobile Accessibility: Nowadays social media is accessible anywhere owing to use of mobile applications. This provides constant connectivity to several platforms.

These features have made social media a powerful tool for personal expression, marketing, and community building. These features collectively contribute to the dynamic and interactive nature of social media, making it a powerful tool for communication, entertainment, and information sharing. It’s important to note that while social media offers many benefits, it also comes with responsibilities and potential risks, such as privacy concerns and the spread of misinformation.

HISTORICAL DEVELOPMENT OF SOCIAL MEDIA

So far the history of social media has been associated with the advancement of communications technology since the late 1800s. A frequent beginning point is Samuel Morse's first telegraph, which he sent from Washington, D.C. to Baltimore in 1844.[17] The internet originated in the 1960s and 1970s, a number of commercial and public organizations sought to develop methods for computers to share information. This can be seen as the birth of internet social media. However, it wasn't until the 1980s, and especially the 1990s, that personal computing devices became more commonplace, laying the stage for the rise of social media.

The history of social media can be divided into three main periods:

1. 1844- Morse's telegraph machine.
2. 1990s- Emergency of Social Media Sites such as SixDegrees.com, Classmate.com
3. 2000s- Rise of modern social media outlets like LinkedIn, Facebook, Twitter, Instagram, etc.

It could therefore be argued that social media probably truly began in 1997 with the establishment of SixDegrees—a short-lived social-networking website for making friends. 1999 saw the rise in Personal blogs with the launch of LiveJournal. And ubiquitous social-media platforms LinkedIn and Facebook rose in early 2000s.[18]

2.2.1 SixDegrees.com

It was one of the earliest online social media sites, and it was named after the concept of "six degrees of separation" which states that everyone in the world is connected to everyone else by no more than six degrees of separation. The six degrees of separation notion is based on the assumption that all living creatures and all that is in the world are six or fewer steps apart, allowing a chain of "a friend of a friend" utterances to connect any two persons in no more than six steps.

---

[17] Morse Code & the Telegraph, HISTORY, A&E Television Networks, August 12,2022 via History.com Editors, https://www.history.com/topics/inventions/telegraph

[18] http://sixdegrees.com/

The site operated from 1997 to 2000 allowing its users to create profiles, list friends, family members, and acquaintances, and invite them to join the network through invite codes. It could be considered a pioneer in the social networking space and paved a way for many of the popular platforms we use today. It was recognized as being the "first online social media" site and is often called the "Six Degrees of Kevin Bacon" theory.[19]

Classmates.com and SixDegrees.com were the first businesses to build social networks using web technologies. When Classmates.com was established in 1995, its primary goal was to facilitate relationships between members of military branches, employers, and high school and college graduating classes. The first real social networking site was SixDegrees.com, which went live in 1997 and let users make profiles, keep friend lists, and message each other privately, a feature which Classmate.com did not have.

2.2.2 Friendster

A couple of years down the line ,the site **Friendster** emerged to compete with Six Degrees in 20002.[20] It was a gaming platform that allowed users to sign up with their email address, make friends, and save them as part of a personal network. Users were able to share videos, photos, and messages with other users, and leave comments on other people's profiles, so long as they were part of each others' personal network- friends.

2.2.3 LinkedIn

It was one of the first social media sites in history founded on December 28, 2002 by Reid Hoffman, Allen Blue, Konstantin Guericke, Eric Ly, and Jean-Luc Valliant. Its focus was and is still on professional networking, allowing people to connect with business and school contacts, as well as companies. Today, LinkedIn is the world's largest professional network with more than 1 billion members in more than 200 countries and territories worldwide.[21]

---

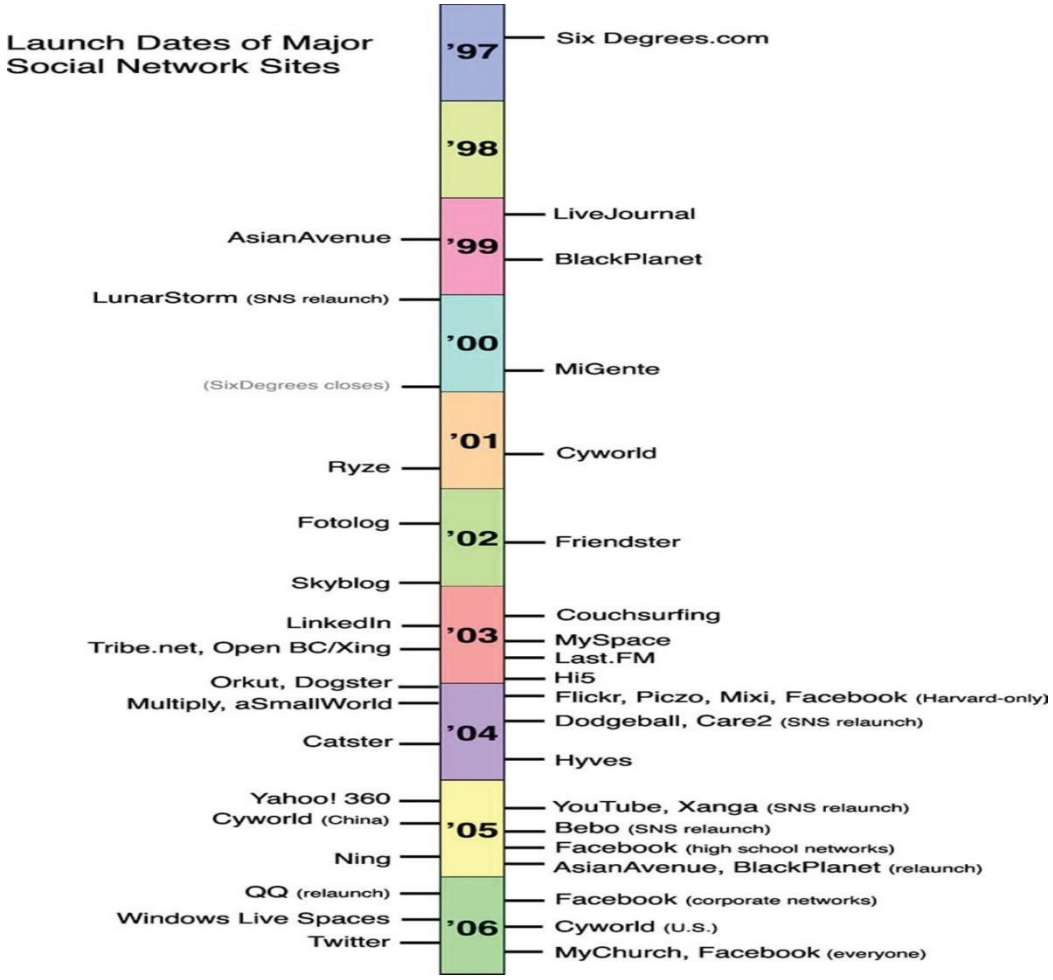
[19] https://newhopeinvestigations.com/blog/the-importance-of-six-degrees-of-kevin-bacon-in-investigations/2020/3/9

[20] Matthew Jones, "The Complete History of Social Media: A Timeline of the Invention of Online Networking", History Cooperative, June 16, 2015, https://historycooperative.org/the-history-of-social-media/

[21] About LinkedIn

2.2.4 MySpace

MySpace was a US social media platform was founded in August 2003 by Brad Greenspan, Chris DeWolfe, and Tom Anderson. It allowed its users to create web profile pages that highlighted their interest while connecting with other members. Users on MySpace used fictitious names and not real ones.



17

Timeline of the launch dates of many major SNSs and dates when community sites re- launched with SNS features.

2.2.5 Facebook

Both a social media platform and a social networking service, it was established in 2004 by Mark Zuckerberg to connect with friends, families and people that shared same interests while discovering new trends. Today it is one of the largest social

networks with billions of users.

2.2.6 X

Formerly known as Twitter, it was developed in 2006 by Jack Dorsey, Noah Glass, Biz Stone, and Evan Williams as a Short Message Service based communication platform. The reason behind creation of twitter was to help friends keep in touch by allowing users to share tweets. Unlike any other social media platform, the text based content shared on X is limited to a certain number of words.

2.2.7 Instagram

Widely known as IG or Insta, it was released in 2010 by Kevin Systrom and Mike Krieger and later acquired by Facebook Inc in 2012. The platform's motto is "give people the power to build and bring the world closer together. IG is basically a photo and video sharing social networking service that allows users to create, share and watch short videos in the form of reels, watch stories and live videos and shop from their favorite brands.The uploaded media that can be edited with filters, be organized by hashtags, and be associated with a location via geographical tagging.

All these social media platforms have evolved with time and society to keep in touch with reality. With advancement in technology, comes along amplified use of these platforms. The fact that they are easy to set up, use and navigate, while seemingly having advantages that overshadow its disadvantages is what draws people to use them. There have been so many cases of privacy violations, cyber bullying and online scams reported from and/or on these platforms.

Sherry Turkle was correct when she said that *"Social media addiction is like a double-edged sword, it can bring both positive and negative effects"* , because at this point, we can all concur that society is now addicted to social media than ever. The amount of users present online today and utilizing technology and internet by way of social media engagement is absolutely insane.

[17] Journal of Computer-Mediated Communication, Volume 13, Issue 1, 1 October 2007, Pages 210–230, https://doi.org/10.1111/j.1083-6101.2007.00393.x

TERMS AND CONDITIONS.

Terms and conditions define the relationship between social media companies and users. However, these legal agreements are long and written in a complex language which is why it remains questionable whether users understand the terms and conditions and are aware of the consequences of consenting to such. Generally, T&C's identify the rights and responsibilities of the parties in a contract. With reference to social media platforms, they form the legal basis of the relationship between the platform and its users.

They among other things, regulate user behavior, content ownership, liability and data usage. Agreeing to the T&C's invokes the right to terminate accounts or suspend user's accounts in case of default or failure to abide by its policies. It's important for users to be aware of the key points in these agreements, as they can have significant implications for privacy, content rights, and more. Understanding the T&C's, will give a user an understanding of how to move forward in case of issues or disputes arising out of use of these network

The T&C's are usually lengthy and written in complex legal language making it difficult for the average user if not all to fully understand its contents. The language in which they are written often times needs someone with legal knowledge to understand them or at least a learned person. Nowadays, they have been reduced to a single word "Agree" which users gladly do without any second thought. This makes one wonder if users truly understand what they are consenting to or even understand the consequences of their actions.

The most common thing that users of social media platforms do is accept the terms of service without reading them, let alone understanding it. When signing up for such a service, users consent by reading or at least scrolling through the terms of service and by clicking the agree button.

- **Terms of Service**: This is the agreement you accept when using a platform

or website. It includes rules about what you can post, how you can interact with others, and the types of content that are prohibited.

- **Privacy Policy**: Details how the platform collects, uses, and shares your personal information. It also explains the data protection measures in place and how you can control your privacy settings.

- **Community Standards**: These are guidelines that outline the dos and don'ts of the platform, what is allowed and that which is socially prohibited such as hate speech, nudity, or violent content. It also provides information on how to report abuse or violations.

- **Intellectual Property**: Social media terms often include clauses about the ownership of content posted on the platform and how it can be used by both the platform and other users.

- **Data Protection**: With the increasing concern over data privacy, terms and conditions also cover how user data is protected and the platform's compliance with data protection laws.

Contractual Nature of T&Cs

Terms and Conditions can be considered a contract between the user and social media platform in the sense that they establish a contractual relationship between the two. Social Media contractual law establishes how privacy, confidentiality, and data exchange are managed under terms and conditions (sometimes called terms of services) and privacy policies. In social media cases, the types of contracts used are called Click-wrap, Browse-wrap and shrink contracts.

Click-wrap contracts are agreements that offers users to accept or decline digitally made policies. Just tike the name suggest they are agreement that acknowledge users' consent to the terms and conditions of a website or application by way of a click. They often apply to online agreements when users download content, make

purchases, or sign-up for an email list.They are the most common agreements used in social media platforms.

According to contract law, a valid contract must consist of offer and acceptance. Social media platforms offer their services and users accept the offer proposed. To accept the offer, the users must show by accepting the terms and conditions of such platforms. Users are expected to actively indicate their acceptance of the T&C's before accessing the content and using the platform by clicking the "Agree" or "I Consent" button in most cases. Sometimes its by accepting to use the platform, that indicates consent and agreement to these terms. In most cases the platform will blatantly state that, if users do not accept and comply with the T&C's, they may not be able to use the Services at all. Its more like a take-it or leave it type of agreement with no room for bargaining. This is also the reason why users end up agreeing an giving their consent without fully understanding the consequences.

A legally binding agreement between the user and the social media platform, the terms of service grant the user the right to use the platform's services in exchange for the user's commitment to abide by those terms. An offer and consent are typically needed for a contract, and the user must proactively indicate compliance by clicking the conditions they agree to. Other social networking sites publish terms of service through a link that is usually located close to the bottom of the homepage, implying approval through the users' use of the platform.

Just like in a contract, social media platforms expects some sort of consideration, can be n monetary or promises basis basis from users. However, if you don't pay, your consideration is usually an agreement to give up some privacy by enabling the website to track how you use it and frequently the internet through the use of tracking cookies and other technologies that help the social media platform better target its online ads. A lot of social media sites also sell the data they gather from your browsing patterns to outside marketers. Your name, phone number, email address, and other personal information may be included in this data.

Users should read and comprehend the terms and conditions of each social media site to make sure they use it in accordance with the rules and to safeguard their own

rights and privacy. Facebook, for instance, emphasizes the use of data for ad targeting and user experience personalization in their terms of service, which include a wide range of topics from personalized advertising to the services they offer. Accounts may be suspended or terminated, among other penalties, for breaking these rules.

One could therefore argue that social media terms and conditions are legal agreements that define the rights and responsibilities of both the service provider and the client. They may include clauses on confidentiality, copyright and usage, equipment and resources, exclusivity, location, payment, and other aspects of the social media marketing services.[22] Social media terms and conditions help to protect both parties from potential disputes and liabilities.

The terms of service are legally binding contract between the user and the social media platform in which the user agrees to adhere to the platform's terms in exchange for the right to use its services. Typically, a contract requires an offer and a consent, where the user must proactively signal their compliance by clicking acceptance of the terms. Other social media platforms imply consent by the users' use of the platform- implied consent.

[22] Social media marketing terms and conditions - Docular

Consent on Social Media Platforms

Consent means voluntarily and willfully agreeing to do something. It might be in response to another person's proposal and the consenting person must of legal age that is to say they must possess sufficient mental capacity to give consent. Consent requires that it should be free of coercion and undue influence. It is important to note that consent can be withdrawn at any point regardless of the nature of the relationship. Consent is a performative action which is the 'voluntary agreement to or acquiescence in what another person proposes or desires'[23]. When "consent is given based on an adequate explanation of procedures and risks involved as well as anticipated outcomes," informed consent necessitates the individual's agency.

According to Professor Heidi Hurd consent works moral magic as it it transforms things that would be illegal and immoral into lawful and legitimate activities. This statement purports that obtaining consent can inherently change the ethical nature of an action. Actions that might otherwise be considered illegal or immoral become justly acceptable and permissible with consent. Courts in deciding their cases have always considered consent as a key factor in determining the legitimacy and morality of actions within the contexts of sexual offenses, contractual disputes among others. When it comes to privacy, consent authorizes and legitimizes a wide of activities data collection, storing, processing, and usage. Consenting therefore creates a new obligation to refrain from complaining about future or possible disappointments or injuries, even if they constitute a moral or legal claim against the injurer.

In her work titled "The Normative Force of Consent"[24], Professor Hurd examines several views of how consent might limit or promote personal liberty. She contends that, while consent does not make all activities moral, it does erase any claim that

---

[23] Lim, V. (2014). Changing trends in informed consent. International E-Journal of Science, Medicine & Education, 8(1), 3–7. https://doi.org/10.56026/imu.8.1.3
Google Scholar

[24] Hurd, Heidi M., The Normative Force of Consent (August 13, 2015). Forthcoming in the Routledge Handbook on The Ethics of Consent, Peter Schaber ed. (Routledge Press, 2016)., University of Illinois College of Law Legal Studies Research Paper No. 15-36, Available at SSRN: https://ssrn.com/abstract=2643657

such behaviors are wrong for the person giving consent, so transforming the moral landscape and modifying others' moral legacies.

Daniel J. Solove argues that most consent is fiction[25] and allowing doubtful or nonexistent consent to be used as genuine consent legitimizes data acquisition, use, and disclosure without justification. Accordingly he contends that there are two approaches to consent in privacy law; the notice-and-choice approach predominately used in the US and the express consent approach in the EU based on the GDPR.

The Notice and Choice approach is based on Fair Information Practices (FIPs), which prioritize transparency, data quality, and security measures. It entails service providers posting a notice of their privacy practices and users will be deemed to have consented to the terms if they continue to use the services in question. It has been called the current paradigm of consent online.[26] The Notice posted by service providers is will consist of terms and conditions or terms of use agreement. The Choice is an action signifying acceptance of the terms, usually by clicking on an "I agree" button, or simply using the website.

The Express Consent approach is based on the provisions of GDPR[27] which requires organization are required to obtain explicit and informed consent from individuals before processing their personal data. This consent must be freely given, specific, informed, and unambiguous, ensuring that individuals have a clear understanding of how their data will be used. This is provided under Art 7 and recital 32 of GDPR. Express consent therefore is any consent that is voluntarily, affirmative ,clearly and explicitly given without any ambiguity.

Section 13 in The Indian Contract Act, 1872 defines consent as when two or more

[25]Solove, Daniel J., Murky Consent: An Approach to the Fictions of Consent in Privacy Law (August 20, 2023). 104 Boston University Law Review 593 (2024), GWU Legal Studies Research Paper No. 2023-23, GWU Law School Public Law Research Paper No. 2023-23, Available at SSRN: https://ssrn.com/abstract=4333743 or http://dx.doi.org/10.2139/ssrn.4333743

[26] Sloan, Robert H. and Warner, Richard, Beyond Notice and Choice: Privacy, Norms, and Consent (March 25, 2013). Suffolk University Journal of High Technology Law, Forthcoming, Chicago-Kent College of Law Research Paper No. 2013-16, Available at SSRN: https://ssrn.com/abstract=2239099 or http://dx.doi.org/10.2139/ssrn.2239099

[27] Consent - General Data Protection Regulation (GDPR) (gdpr-info.eu)

agree upon the same thing in the same sense. Social media platform consent is a crucial moral and legal matter. It is the voluntary and informed consent to share or utilize one's private information, including photographs, videos, and other types of content, online. By clicking the “Agree” button and accepting the terms and conditions, users consent to social media platforms collecting, using and possibly selling their information.

Social media use has increased along with the rise of digital technology, people are using more of these social media platforms where they put they information in large numbers. Even though the terms and conditions specify that in some cases the kind of information the website will collect from you, what they will do with it, this does not guarantee privacy protection at all, if anything it gives them immunity against liability as users will have provided their informed consent to the use of their information.

The use of user data without authorization, has became an increasing problem, particularly when automated technologies like AI-based web scraping bots are utilized to gather data from social media platforms. This presents serious ethical questions since it might result in the objectification and exploitation of people who are more susceptible. The requirement to safeguard the information emphasizes the significance of informed consent.

Social media platforms capture and trade consumer data for analysis, user profiling and for sale to interested parties and is used extensively in marketing. To collect, store, process and resell this data, they are legally required to obtain informed consent. However, users may agree to consent without the ability to comprehend the consequences of what that consent means. The thousands of words that make up the policies are sometimes condensed into the two choices of "Accept all" and "Manage." Since greater user understanding of privacy has a financial impact on firms, it's possible that too complex privacy policies are contributing to uninformed consent.

Cookies can be defined as pieces of data that websites collects and store on your browser. While accepting these cookies helps provide personalized browsing experience, they also promote targeted advertising.

Accepting them have been affiliated with privacy concerns as they can be used to track the user's movements across the platform, collect and store log in and sensitive information. Even the cookies that users accept almost every time they use these platforms are not as safe and harmless as they appear especially if one is using an unsecured website.

Accepting those cookies gives social media networks access to your ip address, network and your data. Information like the website visited, user id, login details, browsing history, location, personal data like name, address and phone number will be easily accessed by the platform you are using after accepting cookies. Sometimes denying to accept these cookies affects your ability to use the site. Hence while accepting these cookies may not be harmful, it grants these platforms your information which s then stored in their databases vulnerable to violations in case data breaches.

Privacy Policy

A policy is the code of conduct that provides guidelines on how workers or users should use the platform and in turn outlines how the users information will be use. Privacy Policy can therefore be understood as a legal document that discloses how a party collects, stores, uses and discloses a customers, client or employees information as the case may be. It generally explains how service providers handle their users information. In this digital era, website or online platforms use the click-wrap way to prove the user's consent to privacy policy. The privacy policy of a service provider is usually found on their about along with the terms of use.

Social Media Privacy Policy explains how social media platforms collect, use, share, retain and transfer information. It also provides an outline of users' rights and allows them to control their privacy like making their content and account private as well as deciding who gets to view their account at large. The information collected by these platforms usually differs depending on what information users post. Like on WhatsApp, privacy settings will allow users to manage whom their information is visible to; their last seen, profile photo, bio and also status.

Users are usually presented with social media privacy policies either during the registration process or when utilizing the network. Often, in order to use the platform's services, users must accept the conditions of the privacy policy. To make educated decisions regarding their online privacy and to understand how their data will be treated, users should check these policies. Furthermore, social media companies must abide by privacy rules and transparent data practices in compliance with governing laws.

The Central Government of India in an attempt to make online engagement and virtual communities safe has made the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, which require intermediaries, including social media intermediaries, to observe, among others,

diligence as under:[28]

I. To publish on their website and app, their rules and regulations, privacy policy and user agreement;

   To inform the said rules to their users and to make reasonable efforts to cause the users not to host, display, upload, modify, publish, transmit, store, update or share, among others, information which belongs to another person, or is obscene, or is invasive of another' privacy, or is insulting or harassing on the basis of gender, or is racially or ethnically objectionable, or encourages money laundering, or promotes enmity between different groups on the grounds of religion or caste with the intent to incite violence, or is harmful to child, or infringes intellectual property rights, or impersonates another person, or threatens the unity, integrity, defence, security or sovereignty of India or public order, or prevents investigation, or violates any law;

II. Upon receipt of an order from a lawfully authorized government agency, to provide information or assistance for prevention, detection, investigation or prosecution under law, or for cyber security incidents;

III. To have in place a grievance redressal machinery, and resolve complaints of violation of the rules within 72 hours of being reported;

IV. In case an intermediary is a significant social media intermediary (i.e., an intermediary having more than 50 lakh registered users in India), to additionally observe due diligence in terms of appointing a Chief Compliance Officer, a nodal contact person for 24x7 coordination with law enforcement agencies and a Resident Grievance Officer, publishing monthly compliance reports.

The privacy policy is in line with GDPR provisions which aims at granting users access to the data that companies or service providers have about them. These privacy policies must be transparent and in compliance with data protection laws. According to this provision, a privacy policy should provide and include the following clauses:

- Kind of information they collect

[28] Press Information Bureau (pib.gov.in)

- How the information is collected and used
- Legal basis for data collection
- Data security practices
- Information about third-party sharing
- User rights
- International data transfers
- Use by children
- Cookies

In support of privacy and data protection, the California Online Privacy Protection Act requires online commercial websites to provide and post their privacy policy. Its so sad however that most people have not forsaken their habit of skipping important guidelines. The same manner users usually skip the T&C's , they also skip over the privacy policy when joining a social network unaware that they can learn a lot of useful information by reviewing a privacy policy before signing up for service.

Issues with Social Media.

The discussions about social media concerns has been a controversial one with a portion of people purporting how beneficial it is and others wailing about the negatives associated with social media. Social media has indeed made a lot of things easier for the society today starting from easy communication, profound and easy access to news, information and content. Despite these, there have been so many concerns surrounding social media usage that perhaps might even override its positive impact in people's lives. Two main concerns that stand out amid the praise for the variety of viewpoints, user creativity, and activism opportunities that young people find on social media is perhaps the negative effects of harmful content and what many young participants refer to as "addictive" platform design on young people's mental health and their sense of helplessness in the face of multinational corporations' persistent prodding to engage in a vicious cycle of sharing personal information and consuming content which is most cases violate their personal privacy.

The use of social media is all good and rosy until people realize that not only are they sacrificing their time but also their mental health, well being, relationships and their identities. From anxiety, depression, stalking, pressure, addiction, insomnia to estranged relationships, studies have shown that most people that engage in social media are affected by one or two of these if not all. People are more present online that physically, emotionally with their loved ones. In a room full of family, friends and loved ones, 90% if not all will be on their phones using social media and engaging online.

While social media is beneficial to users, it has risks associated with its use. The more information is shared online, the more it becomes vulnerable to privacy violations among other issues. Sharing personal information on social media can lead to a number of negative outcomes, such as losing control over our information, being targeted by advertisers, having a higher chance of identity theft and fraud, being vulnerable to online harassment and cyberbullying, and—possibly the biggest risk of all—being singled out by stalkers and predators.

Negative Impact

I. **Loss of control over shared information-** one of the biggest risks associated with sharing personal information on social media is the loss of control over the shared information. The moment a user post something, it becomes difficult control who has access to their post or shared information. Even the user has opted to make the post private, it will be publicized as people will be sharing it among their network. It becomes a friend of a friend situation with friends re- posting, sharing for others to see such that even after deleting the post or restricting access to it, the information already posted will still spread like wildfire. At the end of the day, the information shared ca be used for purposes other than that which the owner intended, including but not limited to nefarious purposes and online fraud .

II. **Targeted Advertisement-** sharing information online makes it easier for advertisers and data miners to use that information to target you with ads and other marketing materials. Most social media platforms rely revenue generated from targeted advertising, so they often collect, retain and transfer the information users share on their platforms advertisers and data miners. The more information user share on social media, the easier it is for advertisers and data miners to create a more detailed profile and target users with ads that are tailored to suit their interests. While this might be harmless and beneficial in some cases, it can also be intrusive and in violation of user's privacy.

III. **Risk of Identity Theft and Fraud-** perhaps the most dangerous and biggest risk of sharing personal information on social media is becoming vulnerable to identity theft and fraud. Identity theft is when a third party gains unauthorized access to your PII and begins to use it to commit crimes mostly for financial and personal gain. This type of a crime typically happens when a person illegally obtains personal and confidential information of another persons and uses it to for personal gain which in most cases will be criminal. Identity theft has been in other cases referred to as Data theft which involves hacking of confidential data like credit card numbers, bank details to obtain money or commit heinous crimes. This could be a result of data breaches as platforms store data indefinitely on multiple internet platforms.

Identity theft is India is punishable under section 66c of the IT act, 2000 which provides that;

"*Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine with may extend to rupees one lakh."*

Examples of identity theft and fraud include: impersonation, hacking to scam and malware.

a) ***Impersonation*** is when someone with malicious intentions uses someone's online identity in order to gain financial benefits such as obtaining a loan in their name or defraud their family and friends for money, or with the purpose of harassing, intimidating, or threatening their victim. Hackers can exploit personal information like name, address, phone number, and date of birth to impersonate users and defraud a bank or credit card business. This allows them to acquire access to users' financial accounts and steal their money, or to take out a loan in their names and leave them in debt.

This criminal act is punished under section 66D of the IT Act,2000 which states that;

"Whoever, by means for any communication device or computer resource cheats by impersonating, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees."

b) ***Scams*** is when hackers send emails or messages that appear to be from a legitimate website or firm requesting users' to enter their username and password, granting the hackers access to login information

c) ***Malware*** refers to when hackers use the information users' share to send malicious software such as viruses disguised as links or attachments in emails or messages so that when users open the attachment or click on the link, the

virus can be installed on their device without their knowledge, giving the hacker access to their personal information

Cyber- bullying- again disclosing personal information online makes one vulnerable to being targeted by stalkers or predators. Online stalkers utilize the internet to discover possible victims, frequently focusing on those they believe they can manipulate or who are vulnerable in some way. They do so by scouting social media platforms for personal information that may allow them to identify and contact their targets. This can include information on their victims' whereabouts, personal information, and even everyday activities or habits. After identifying a possible victim, they may use the information to track their activities online or in person.

Looking at all the above mention risks associated with social media usage, we can concur that the disturbing concerns are all stemming from privacy.

Positive Impacts of Social Media.

"Social media is the fastest way to spread ideas"

-Evans Williams.

Social media platforms have revolutionized the way ideas and information are being disseminated owing to technological advancements. Today information is easily accessible and rapidly shared to reach a large number of people across the globe. Social media supports instant online discussion, businesses are blooming and can easily discover new customers online. Payments are being done digitally online, for example, PayPal, PayTM among other digital financial platforms.

An invaluable advantage of using social media today is that its easy to locate user owing to long time maintenance of user profiles. As stated earlier, information shared on this platform is kept for an indefinite period of time which makes it easier to locate a friend, family member or any user at all. Bolanos F et al used Facebook from 2009- 2011 to find and re-contact participants eight years after enrollment in a study about methamphetamine use to invite them to participate in a second study.[29] Nine percent of those participants were reached via Facebook and likely would not have been located by conventional methods

- **Instant Online Discussion:** people use social media platforms like Reddit, Twitter, and Facebook Groups to participate in online discussions and post question about any topic. Instagram does this through live videos or the new feature of note on the users' profile. Users' can also post question on their stories and engage with their followers based on that. Nowadays people have taken interest in anonymous confessions whereby a user will ask they followers a question with the catch that their replies will be anonymous. Basically, social media has made communication so easy.

- **Knowledge Sharing:** Social media facilitates global knowledge sharing as

[29] Bolanos F, Herbeck D, Christou D, Lovinger K, Pham A, Raihan A, Rodriguez L, Sheaff P, and Brecht M-L. 2012. "Using Facebook to maximize follow-up response rates in a longitudinal study of adults who use methamphetamine." Substance abuse: research and treatment 6:1–11. doi: 10.4137/SART.S8485 [PMC free article] [PubMed] [CrossRef] [Google Scholar]

users can share their expertise with others and learn from them. People can easily share their knowledge with a wide range of audience, post quizzes and sometimes give prices in the form of giveaways to winners. Recently language experts have been teaching ad sharing content online like teaching language to their followers; especially English, Korean and Chinese.

- **Keeping in Touch:** With societal changes, people moving to different place and possibly losing contact to keep in touch, social media bridges the physical distance. The concept of loosing contact has long became a folktale and a foreign practice as people can stay connected with old friends, even through video or audio calls, maintaining valuable relationships with the help of social media.

- **Reducing Stigma:** Social media provides education about diverse conditions and classes of life. It gives a feeling of togetherness and equality to all without discrimination. This helps reduce stigma related to survivors of rape, disability, mental health, race, sexuality, and identity. It fosters understanding, acceptance and support.

- **Generating Revenue:** People nowadays use social media platforms to reach their targeted audience and advertise their products, goods and services. Most businesses are being conducted on these platforms. People have business pages to showcase their works and draw customers with online reviews

Social Media Platforms and Networks have now became an integral part of our lives, pivotal at that. Everything revolves around social media from communication to doing business, people have been utilizing this tool successfully but not without any concerns. While we cry about the dangers of social media, we should not forget to appraise it for its contribution so far.

CHAPTER 3

CHAPTER 3- FACEBOOK AS A SOCIAL MEDIA PLATFORM

Facebook is a social media and social networking service owned by the American technology conglomerate Meta. As a brain child of Mark Zuckerberg et al, it was created on February 4th 2004. It started as a platform for Harvard students but later expanded to all. As of today, facebook is one of the most popular social media platform where people connect with friends and family, share photos, videos and do pretty much everything one can do through social media.

Facebook presents a platform for users to interact and communicate with each other from all the corners of the world. It features a very interactive interface which allows the users to view and post pictures, videos and other forms of media.
In its early years, an offer of 1 billion was made to the creators of Facebook by Yahoo Inc in 2006, but it was rejected. The company was later made public 6 years after this offer in 2012.[30]

Facebook has been around for quite some time now and most analysts have predicted its demise only to be shocked by Facebook's perseverance. After the creation of Facebook numerous social media companies have been created. With today's fast pace it was almost inevitable that people would dessert Facebook. However, that has not been the case, the newer apps have fought to replace each other and left Facebook unscathed.
Facebook boasts of holding a position of certain dominance over the other social media platforms. This advantage is owed to a number of factors which include;

1. **Ease to use**- Facebook, maybe owing to it's dated origins, is simpler to use and thus, many people can use it. The old population can easily use Facebook because it was from their time and the younger generations can easily use it because it has less complex commands.
2. **Group and Community feature** – the community feature of Facebook allows for users to connect with other users who share the same interests or the same beliefs. Group activities are essential for social media platforms as

[30] Ibid

they keep the users actively engaged.

3. **Cross-platform interference** – Facebook, under the Metaverse, can connect with other social media platforms such as WhatsApp and Instagram. This offers a sense of continuity to the users. This allows them to access or share media or messages from one social media platform to another easily.
4. **Marketplace and e-commerce** – Facebook boast of a market which connects the seller to the buyer directly. Facebook marketplace offers a market for a wide range of products and service which one can access at his/her own time and find the best price which suits them. This feature has been enjoyed by many of the users hence its popularity.
5. **New Features and Updates** – understanding the need of new customers and changing trends, Facebook regularly introduces new features such as Facebook live and 360 degree photos. This keeps the users hooked and allows for improvements from Facebook.
6. **Advertisement** – Facebook offers a large platform for advertisement of goods and services which attracts both, the brands willing to sell their products and the consumers ready to buy the products.

Meta's market cap stands at $1.19 trillion as of mid-February 2024, and it reported 3.19 daily active people for all its platforms in December 2023. Advertising comprised 97.8% of the company's total revenue in 2023. Facebook alone accounted for 2.11 billion daily active users in the fourth quarter of 2023.[31]

The competitive advantages of Facebook are steep: its sheer number of users compared with LinkedIn (930 million users as of 2023) and X (353.9 million users worldwide estimated for 2023) means it can introduce new products or lead users across its platforms with far less effort than the monumental advertising campaigns others would need to launch such products.[32]

Facebook as a social media platform has presented an advertising platform which is undeniably large and far reaching. Various companies and brands tend to utilize this

[31] https://www.investopedia.com/articles/company-insights/070216/what-facebooks-advantage-over-other-social-media-fb.asp
[32] Ibid

platform for the promotion of their products and services. However, this has led to a new variant of issues in the name of data farming.

Privacy Related issues with Facebook

From its date of creation till date, Facebook has faced severe backlash due to privacy concerns on the platforms. User's have had issues ranging from unauthorized sharing of their personal information, data breaches, tagging without permission, stalking to harassment.

- **Unauthorized sharing of personal information:** This refers to disclosing someone's private information, such as contact information, financial information, or sensitive personal data, without their permission. While Facebook prohibits user's from posting and sharing their personally identifying information, it is inevitable that such information will end up on the platform. The information on the platform can be shared by the corporation to its third parties like law enforcement agencies, civil litigants or by friends and user's themselves. The knowledge by user's that their information will and can be shared to others does not equal to consent. Hackers can also obtain user's information and share it to the dark web without their consent.

- **Tagging without permission:** Tagging someone in a post or photo without their permission violates their privacy, especially if the topic is sensitive or improper. You can be tagged in posts and photos by Friends, friends of friends or even strangers. Most facebook user's have at one point faced this issue wherein they were tagged in usually most obscene post by strangers of even friends that might have been hacked. While this can be reviewed and rectified by deleting the post, these posts can be deleted from the user's timeline but may appear in Feed and elsewhere on Facebook. Facebook provides an opportunity to user's to manage the tagging settings and notifies them when someone them.

- **Stalking or harassment:** Constantly monitoring someone's profile, sending unwelcome messages, or indulging in online harassment violates privacy and may result in legal action. Facebook stalking is a branch of Cyberstalking which can be defined as using the Internet, email, or other types of electronic communications to stalk, harass, or threaten another person. Facebook stalking

or harassment can therefore be defined as frequent unwarranted contact over facebook with an intent to cause harm.

- **Fake profiles:** Creating a phony profile to impersonate another person or deceive others can also be a violation of Facebook's terms of service.

- **Data breaches:** If a user's account is hacked or if Facebook experiences a data breach, it can result in unauthorized access to personal information, compromising privacy. A data breach also known as security breach or data leakage can be defined as when unauthorized individuals gain access to confidential information.

The information stored on Facebook data base is vulnerable to data breaches which in turn is harmful to user's as their information can be misused. Hackers can use compromised data for illegal activities including identity theft, financial fraud, spamming or even extortion. One notable data breach facebook had to deal with was the 2018 Cambridge Analytica scandal wherein Cambridge Analytica, a political data business hired by President Trump's 2016 election campaign, obtained information on 50 million Facebook users in order to identify American voters' personalities and affect their behavior[33]. This raised questions about how the social media conglomerate protects user's information.

The data obtained during this fiasco included information about users' identities, friend networks, and "likes." The idea behind this was to map personality traits based on what individuals liked on Facebook and use that to target audiences with digital adverts. during the investigation, Facebook insisted Cambridge gaining access to user's information was not an act of data breach as it occasionally allows researchers to have access to user data for academic purposes. Facebook supported its claims by arguing that users consent to this access when they create a Facebook account. Arguing that user's consent to such actions enforces the questions as to whether they truly understand their consenting actions and what are the consequences for the same.

[33] Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens - The New York Times

In 2019, Facebook had a security breach that exposed the personal information of over 50 million user's. This happened when the social media giant introduced its view as feature as a way to see how a user's profile looks to other people. According to Guy Rosen, Chief Information Security Officer, there were multiple bugs in this feature that allowed hackers to steal Facebook access tokens and use them to take over people's accounts. Third parties like hackers exploited the vulnerability of this feature to gain access to users' accounts.

The privacy policy of facebook explains their data sharing practices with third parties like civil litigants, law enforcement agencies, external researchers or even their partners. While they claim not to sell the user's information to anyone, they still share it with others third parties in response to legal requests, to comply with applicable law or to prevent harm. but how can user's be sure that their information shared will not bring harm to them. this makes it hard to discern exactly the kind of information that Facebook with others.The 2011 Federal Trade Commission's case against Facebook is a very good example that the masses have absolutely no idea as to what facebook protects and shares with others while abiding with its privacy policy. The FTC charged the social media giant for violating its privacy promise to users by allowing private information to be made public without warning. It was argued that Facebook falsely claimed that third-party apps were able to access only the data they needed to operate when in fact, the apps could access almost all of a user’s personal data. Even if a user did not approve such, a third-party app could still have private posts information collected if their friends used app. Facebook was also charged with sharing user information with advertisers, despite a promise they wouldn’t. Jon Leibowitz, the then chairman of the FTC stated that Facebook as a social media company is obligated to keep the promises about privacy that it makes to its users.

These incidents highlight the importance of safeguarding personal information online and the need for platforms like Facebook to enhance security measures to prevent data breaches. The data breaches so far have made it hard for Facebook to convince lawmakers in the US and beyond, that it is capable of protecting user data. The increasing incidents of privacy violations on Facebook and everywhere else in general have made its protection a serious concern for not only users but also

legislators globally. The US's FTC while addressing the privacy and data usage notified the Facebook Inc. and WhatsApp Inc. in line with the acquisition plans that the privacy commitments of both the corporations' users were to be honored despite the acquisition.[34]

Legal Privacy Cases Against Facebook

"The FTC began investigation the company back in March of 2018 after allegations that Cambridge analytica, the now defunct British political consulting firm had accessed the data of over millions of Facebook users and that information was then used to profile, target and influence voters during political campaigns including the 2016 US Presidential election and the UK's Brexit referendum. Now the focus of this investigation was whether Facebook had violated an agreement stemming from a previous FTC probe to better protect user privacy and according to US media report, the FTC found that was the cases and approved the penalty in a three-to-two that broke along party lines. Republicans were in favor and Democrats were against. Five billion dollars seems like it is indeed a lot of money, but there are those that say it simply does not go far enough, that it's just a small fraction of Facebook's profits.

> A company who earned a little over fifteen billion dollars in its first three month of this year alone, and it is also worth pointing out as well that size of this fine is in line with what Facebook was expecting, indeed its hold investors back in April had put aside most of the money so it's unlikely to feel too much of an additional financial strain as a result and that has to some criticism with critics referring to this fine as a mosquito bite, a parking fine and even an early Christmas present for Facebook."[35]

This was the news report delivered by Dominic Politis, a news reported for CBC News. This serves as a summary to how Facebook exploits its users privacy for its own economic gains, political gains, or even social gains. It also shows who tends to benefit from such exploitation of users privacy infringement. Ultimately, it shows

---

[34] Letter From Jessica L. Rich, Director of the Federal Trade Commission Bureau of Consumer Protection, to Erin Egan, Chief Privacy Officer, Facebook, and to Anne Hoge, General Counsel, WhatsApp Inc. – Reminding Both Firms That WhatsApp Must Continue To Honor Its Promises To Consumers With Respect to the Limited Nature of the Data It Collects, Maintains, and Shares With Third Parties (ftc.gov)

[35] https://youtu.be/-BI0W8dBH-g?si=IZPz8iMY2YKsYAG2

how that the penalties, fines or other actions have hardly any chance of causing any grave danger to the exploitive social media platforms especially bigger ones, in the name of Facebook.

After two years of the birth of Facebook, in 2006, the company faced user outrage when it introduced its News Feed. A year later it had to apologies for telling people what their friends had bought. Years after that, the Federal Trade Commission stepped in – and is now looking at the company again. Facebook has a history of running afoul of regulators and weathering user anger, all the while collecting record profits and racking up more than 2 billion users. [36]

Facebook's loose handling of how it's data was acquired by app developers has plunged the company into the biggest crisis of its 14-year existence. The revelation that a data analytics company used by Donald Trump's presidential campaign was able to surreptitiously collect data on 50 million people through a seemingly innocuous quiz app has forced CEO Mark Zuckerberg to issue a public apology and promise change.[37]

Below is a timeline of how Facebook violated the Privacy policy and its response:

1. News Feed Issue

Date: 2006 September

Issue: Facebook debuted News Feed

Facebook's response: tells users to calm down.

On the 5th of September 2006, Facebook introduced News Feed. This new feature was

[36] Nbcnews.com/tech/social-media/timeline-Facebook-s-privacy-issues-it's response-n859651
[37] Ibid

aimed at lifting the burden of browsing through friends profiles to see if they had changed anything. It was a curated feed which provided a central destination instead of the tiresome browsing. Despite what they put forward as the objective of this new feature, not many of its 8 million users welcomed this feature.

Arguments presented by those who were not in favor of this new feature was that it was too intrusive. This was the view of an estimated one million of the then 8 million users. One would think that the number was too large not to warrant a response but Facebook stayed the course.

2. Beacon Issue

Date; 2007 December

Issue: the first instance of Facebook clashing with advertising privacy issues. Beacon

Facebook's response: the CEO of the company, Mr Zuckerberg apologized and gave the users an option to leave.

There was once a time when companies could track purchases by Facebook users and then notify their Facebook friends of what had been bought … many times without any user consent. [38]

In his apology the CEO of Facebook stated that, "We were excited about Beacon because we believe a lot of information people want to share isn't on Facebook, and if we found the right balance, Beacon would give people an easy and controlled way to

[38] Ibid

share more information with their friends,".[39]
This statement, understanding that Facebook was initially introduced for use by a few number of people, seems innocent enough.

However, putting the estimated 8 million plus users who were now using the social media platform coupled with the fact that at that time Facebook was engaged in talks about advertising and online privacy it seems to be a contemplated economic move. A closer look on the supposed apology given by the CEO, shows the intention to "share more information with friends". This should have gone down as a miscalculation, if anything. The fact that the platform had over 8 million users should have sought to at least consider the possibility of "friends" mixing with strangers and risking the theft or loss of private information only meant for a selected few or family members only.

3. FTC privacy charges

Date: 2011 November

Issue: settling of the FTC privacy charges by Facebook

Facebook's response: Facebook agree that, for the next 20 years, it would undergo independent privacy evaluations annually
Under the Order proposed by FTC, Facebook was:

- Barred from making misrepresentations about the privacy or security of consumers' personal information,
- Required to obtain consumers affirmative express consent before enacting changes that override their privacy preferences,
- Required to prevent anyone from accessing a user's material more than 30 days after the user has deleted his or her account,
- Required to establish and maintain a comprehensive privacy program

[39] Ibid

designed to address privacy risks associated with the development and management of new and existing products and services and to protect the privacy and confidentiality of consumers information, and

- Required, within 180 days, and every two years after that for the next 20 years, to obtain independent, third party audits certifying that it has a privacy program in place that meets or exceeds the requirements of the FTC order, and to ensure that the privacy of consumers' information is protected.[40]

4. Facebook bugs

Date: 2013 June

Issues: private contact information was exposed by a bug on Facebook.

Facebook's response: Facebook notified the people whose information was exposed that it had fixed the bugs.

The bug had exposed the private information of 6 million Facebook users. The bug sent out the phone numbers and email addresses of these users to any one who had any remote connection or link with the affected users.
Information such as phone numbers or emails or any other contact information is considered private information as it is the digital address of people online.

5. Mood manipulation experiment

[40] epic.org/Facebook-2011-ftc-consent-order/#:~:text=This%20was%20the%20first%20fine,practices%20that%20violate%20user%20privacy.

Date: 2014 July

Issues: An experiment on mood manipulation on Facebook users.

Facebook's response: the data scientist of Facebook apologised.

The mood manipulation experiment on Facebook included changing the newsfeed of 500 thousand selected Facebook users to show more negative or positive posts. The experiment was targeted at highlighting how emotions could be spread on social media. The results were published in the proceedings of the National Academy of Sciences, kicking off a firestorm of backlash over whether the study was ethical. [41] The Facebook data scientist, Adam D.I Kramer, who led the experiment, issued an apology four years later stating, "I can understand why some people have concerns about it, and my co-authors and I are very sorry for the way the paper described the research and any anxiety it caused,".

6. New Apps draining private information

Date: 2015 April

Issues: Applications which were draining private information were cut off by Facebook.

Facebook's response: please keep building apps.

In 2014, Facebook cited privacy concerns and promised it would limit access to developers. But by the time the policy took effect the next year, Facebook had one big issue: it still couldn't keep track of how many developers were using previously downloaded data, according to current and former employees who spoke with The

[41] Ibid

Wall Street Journal. [42]

This was the first fine against Facebook since EPIC and a coalition of privacy organisations filed a complaint with the Commission about the company's business practices back in 2009. The FTC fined Facebook 5billion USD, but required no meaningful changes to the business practices that violate user privacy. [43]

7. Facebook tracking Belgian users on the internet

Date: 2018 February

Issue: Facebook was told to cease tracking people across the entire internet by the Belgian court.

Facebook's response: the court's ruling was appealed by Facebook.

Collection of private data of Belgian users, through the use of cookies by Facebook was ordered to be stopped. Facebook was ordered to delete all illegally collected data from Belgian users and others related or risk a fine of up to 100 million Euros. Facebook said it had complied with European data protection laws and gives people the choice to opt out of data collection on third party websites and applications. The company said it would appeal the ruling.[44]

8. Facebook data theft

Date: 2018 March

Issue: It was uncovered that Facebook knew about the massive data theft but did nothing.

---

[42] Ibid
[43] epic.org/Facebook-2011-ftc-consent-order/#:~:text=This%20was%20the%20first%20fine,practices%20that%20violate%20user%20privacy.
[44] Ibid

Facebook's response: Policy changes and an apology tour.

The issue was addressed by Facebook's CEO, Mark Zuckerberg. He posted the word "sorry" on his Facebook wall.
Belayer addressed the issue with a published statement, where he stated, I've been working to understand exactly what happened and how to make sure this doesn't happen again. The good news is that the most important actions to prevent this from happening again today, we had already taken years ago. But we also made mistakes, there's more to do and we need to step up and do it.".[45]

9. Clashes with FTC

Date: 2019 July

Issue: The US Federal Trade Commission has announced a potential deal to close its inquiry into Facebook.

10. EPIC issues

Date: July 26 2019

Issue: EPIC makes an application to intervene in the United States vs. Facebook case to safeguard the rights of Facebook users.

EPIC filed a complaint concerning Facebook's secretive and non-consensual use of personal information.[46]

Case Laws

Smith v. Facebook

[45] Ibid
[46] https://www.google.com/url?q=https://epic.org/documents/epic-v-ftc-facebook-assessments/%23:~:text%3DIn%2520In%2520re%2520Facebook%2520(Psychological,in%2520In%2520re%2520Facebook%2520(Facial&sa=U&sqi=2&ved=2ahUKEwiAgL-jwK-GAxXmxTgGHcbMBfYQFnoECBYQBQ&usg=AOvVaw1LPp6b2Jhwme5czuc1eEL3

This case was based on whether Facebook's tracking of user's visits to medical websites violated California and Federal privacy laws.[47]

Factual background

This class action complaint is about Facebook's surveillance of its users every time they explore third-party websites. The plaintiffs in this case claim that when they visited specific health-care-related sites, Facebook was able to directly identify and monitor them using the "share" and "like" buttons included on the page. When a third-party website incorporates these buttons, Facebook can personally identify users to that website using three methods: (1) acquiring that person's IP address, (2) placing cookies on that person's browser, and (3) utilizing a process known as "browser fingerprinting." Facebook can then track users every time they browse the third-party website, collecting personal information that it can sell to marketers or use to target specific adverts.[48]

In this lawsuit, the plaintiffs claimed that Facebook was able to monitor individuals as they viewed health care websites and obtain highly confidential data about them. Federal law imposes greater restrictions on the collecting of health care-related information compared to what it imposes on other sensitive data and the plaintiffs have alleged that both Facebook and the Health care Defendants failed to meet this burden.[49]

Plaintiffs further claimed that the tracking violated their right to privacy under the California Constitution, as well as the Wiretap Act and California Invasion of Privacy Act.

Lower Court Ruling

The defendants' motion to dismiss the plaintiffs claim was granted by the District Court for the Northern District of California. This decision was founded on the opinion that

[47] https://epic.org/documents/smith-v-facebook/
[48] Ibid
[49] Ibid

the the claimants' rights had not been violated since Facebook's Terms of Service hindered them from initiating claims for privacy under California and Federal law. Facebook's Terms of Service state, "We collect information when you visit or use third-party websites and apps that use our Services (like when they offer our Like button or Facebook Log In or use our measurement and advertising services)."[50]

Comment on Case

This case serves as an example of how the users are not reading and understanding the terms and conditions of social media platforms, Facebook. This results in such cases which do have violations but can not be acted upon owing to the terms and conditions that users blindly agree to.

More importantly, this case serves to show how the social media platforms draft up water tight terms and conditions which are aimed at misusing users private information. The terms and conditions are fully prepared to quash out any outcries in regards to personal information, showing that the social media platforms intentionally set up predatory terms and conditions which in turn entrap users who blindly agree and accept these conditions without even reading them.

The Smith v. Facebook case was one which was already won based on facts. The terms and conditions of Facebook seem to have been written in anticipation of such an issue. The terms and conditions are usually written or announced in a different way as compared to how the rest of the product is presented. Be it the smaller font, faster paced announcers or back page positioning of the terms and conditions, the users have been wired into thinking that they can just agree to the terms and conditions at no costs. Such is the same case with the terms and conditions of social media platforms. They hide heinous crimes and violations which the user's are not suspecting which in time harm them in the long run.

The case was an open-shut-case as the plaintiff had consented and agreed to the very same terms and conditions which were against him. The respondents duty was only to show how and where the plaintiff gave his consent, and he could not have had an easier

[50] Ibid

task.

All this is to show how important it is to review and understand terms and conditions before agreeing to them. Have a lawyer or your consultant read and understand the terms and conditions before he advises you on the best course of action.

Karmanya Singh Sareen v. Union of India.

On September 6, 2017, the Supreme Court obligated both WhatsApp and Facebook to provide affidavits clarifying what data is exchanged by them, that had been promptly submitted by the respective respondents.[51]

Issues raised and arguments presented

The motion presents a solution to the ongoing issue of internet privacy and urges that authorities aid in ensuring the safety of personal information. Currently, India lacks explicit data privacy regulations. The petition addressed the following issues: [52]

Does Whatsapp's Privacy Policy violate its users' personal liberties?
Shouldn't Facebook provide information choices for those using it?
Is the process by which WhatsApp obtained consent from users enticing?

Arguments by the petitioner

The grounds for the respondent's action, as asserted in the present writ petition, is that the present proposal in the privacy terms of "WhatsApp" would result in a modification of the most vital, fundamental, and key elements of "WhatsApp," which is adequate safeguarding of the privacy of its user groups' personal data and information. This subsequently infringes on the fundamental right to privacy provided by Article 21 of the Constitution.[53]

Petitioners argued Privacy is a legal right, thus the government must control data

[51] https://blog.ipleaders.in/karmanya-singh-sareen-union-india-whatsapp-facebook-privacy-case/#Why_was_the_PIL_filed_in_Delhi_High_Court
[52] Ibid
[53] Ibid

exchange and pass policies to preserve one's privacy. References to other nations that have implemented steps to share data were relied on.[54]

Arguments made by the respondent using affidavits.

WhatsApp provides privacy, complete anonymity, and additional safety tools. It does not retain messages from users after they are officially received. Whenever conversations between users are encrypted throughout their entirety, WhatsApp and other parties cannot access them. WhatsApp does not archive communications in the normal course of providing services to its users. WhatsApp deletes messages (including chats, images, videos, voice messages, files, and shared location information) after they have been delivered.[55]

WhatsApp also provides end-to-end encryption for its products and services, which is enabled by default whenever users and those who receive messages using WhatsApp software versions published after April 2, 2016. Because conversations between users are end-to-end encrypted, WhatsApp and other parties cannot access them.

Users may delete their WhatsApp account at any time (including if users want to revoke their consent to WhatsApp's use of their information) using WhatsApp's in-app 'delete my account' feature. When a user deletes his/her WhatsApp account, his/her undelivered messages are deleted from WhatsApp's servers as well as any of the user's other information WhatsApp no longer needs to operate and provide the WhatsApp services.[56]

[54] Ibid
[55] Ibid
[56] Ibid

CHAPTER 4

CHAPTER 4- LEGAL LIABILITY

Understanding the Fault

"Fault-finding without suggestions for improvement is a waste of time ." Ralph C Smedley.

As boldly as the statement suggests, the need for an improvement is indeed the only hope in resolving this privacy violation issues. However, this is not to neglect the fact that the fault and it's bearer are to be found first.

Innocent victim or background contributor? Facebook now faces questions from authorities on both sides of the Atlantic Ocean after news reports in The Guardian and The New York Times this week revealed that a psychologist illicitly gave data from 50 million Facebook users to a political consulting firm that tailored political ads to many users during the 2016 U.S. presidential election.[57]

It is undeniable that the privacy issue has a root cause, a party at fault, who triggered the situation. It is understandable that with every right, a duty is born. The price of enjoying a right is observing a duty. The right to privacy is no exception to this law. With data privacy and protection, the users are supposed to be careful not to give away vital personal information easily to untrustworthy platforms. This does not excuse the social media platforms as they need to adhere to the rules and regulations put in place to manage personal information or data. They should also avoid predatory terms and conditions for users.

Undeniable, the social media platforms are supposed to adhere to regulations and guidelines in place when handling personal information or data be it in storage, collection, transferring or processing, but this is not to say the users are free to be negligent. Ignorant and negligent users are a more dangerous force against themselves than they realize.

The unauthorized use of personal information belonging to users of apps integrated with the Facebook platform affects millions of users. Crucially, although privacy concerns and

[57] https://news.harvard.edu/gazette/story/2018/03/facebooks-privacy-problem-may-erode-web-trust-harvard-analyst-says/

awareness have increased, the use of these apps, and related privacy behaviors, remain largely unchanged. Given that such privacy behaviors are likely influenced by individuals' personality traits, it is imperative to better understand which personality traits make individuals more vulnerable to such unauthorized uses.[58]

This chapter sets course to discover who is truly to blame in the privacy violation issues between social media platforms, especially Facebook, and the users of the said social media platforms.

Facebook's Fault

Facebook can not steer clear of the responsibility when it comes to invasions on its home grounds. One user argued that within a span of two weeks, Facebook traced them across roughly 95 distinct mobile applications, internet pages, and companies, and those constitute only a few they were aware of. "It seemed as if Facebook had hired a private investigator to write a record about my life," he says.[59]

Facebook may be free, but you pay for it with your privacy. And Facebook keeps raising the price.[60]
Such is the nature of complaints against Facebook.

The size of Facebook and the channels in which it is involved in are causes of concern and surely suggest that Facebook is at fault in the Privacy violation issues. A reporter of the Washington Post said, "Facebook has become too big to escape. We're rightly becoming more skeptical of Big Tech monopolies, and that should include the sheer volume of data they collect." This serves as an indication of how Facebook is abusing its size in the privacy violations.

Facebook drafted Terms and Conditions which provided solace when the Social media giant was questioned about its privacy policies. This shows the premeditated predatory nature of the terms and conditions that Facebook presents to the people.

---

[58] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7452521/
[59] https://www.washingtonpost.com/technology/2021/08/29/facebook-privacy-monopoly/
[60] Ibid

Another factor which supports that the privacy violations are Facebook's fault is the fact that the Terms and conditions drafted by Facebook blatantly state that the harvest and sale off the user's personal information. In the case of Smith v. Facebook it was stated that the policies in the terms and conditions stated that, "We collect information when you visit or use third party websites and apps that use our Services (like when they offer our like button or Facebook log in or use our measurement and advertising services)."[61]

The privacy violations are Facebook's fault. This is owing to the fact that Facebook deliberately enters into agreements with third parties who then turn out to be somehow in possession of users personal information or data only submitted on Facebook. If Facebook had chosen to limit its involvement with third parties, the case would have been avoided all together.

Facebook is involved with various third party applications which depend on person information for effective audience targeting. Facebook is aware of this and still chooses to work with them. This shows howFacebook is willing to, at the most opportune time, engage with them in business while violating privacy rights of billions of users.

The User's Fault

Notwithstanding ongoing privacy concerns (e.g., Cambridge Analytica), many people continue utilizing Facebook (Acopio and Bance, 2016; Hatzithomas et al., 2017).[62] If it has been brought to court with issues regarding to violations of privacy, how wise is it to insert your personal information into?

This is especially clear in the case of Cambridge Analytica, which exploited Facebook to gather the psychological attributes of countless its users. (Pegg and Cadwalladr, 2018).[63] Yet users kept flooding the social media platform, Facebook. What would you expect from a social media platform which has been charged for privacy violations?

[61] Ibid
[62] Ibid
[63] Ibid

Simple, privacy violations. To expect anything else would be unhinge dementia at its highest level.

The users are more to blame as they have privacy settings which they can make use of in protecting themselves against social media platforms. If an option to protect oneself or to limit the damage to oneself, it is better to be equipped with a defence than to have none at all.

Another fact that makes the users more to blame is that in most cases, the users are prepared to exchange their privacy for social media services. A new study has demonstrated that this is becoming increasingly prevalent across societies as individuals are motivated to satisfy their information and social requirements at the cost of their privacy (Pentina et al., 2016). Thus, if the users value information and social needs above their privacy then the fault is theirs.

Ignorance and negligence is a crucial factor which makes the Facebook privacy violations cases, the users fault. Firstly, the terms and conditions of Facebook clearly state how they operate and how it will affect the users, but the users do not read these conditions which are designed as warnings. Same goes with the Facebook policies, just browsing those policies would have you in a better path but the users do not pay heed and instead pay the price.
Secondly, the privacy settings are built in these social media platforms or at times are provided by third party applications. Yet users chose to engage social media platforms like Facebook without any data protection.

In the case of Smith v. Facebook, the plaintiff had not read the terms and conditions which ultimately led to the dismissal of his case. The policies of Facebook stated that, "We collect information when you visit or use third party websites and apps that use our Services (like when they offer our like button or Facebook log in or use our measurement and advertising services)." This policy meant that all the other defenses they were entailed to were washed away.
If the users had read and understood this policy it is likely that they would have made a better choice in regards to their personal information. Thus, again the user is to blame for the violation of his/ her own privacy rights.

Consumers are more into free media than being concerned about their privacy. It is important to note that at most times, it is the user-generated content that haunts people and compromise their privacy in a way that if other social media users spread offensive information; which they often do, one can make claims of unlawful invasion of privacy under torts for civil liability. That being the case, the social media giants will however have no direct liability if not at all for user generated invasions. Users therefore must do away with entitlement and misguided and misdirected privacy violations. It all starts with them- owners of information.

Third party Application's fault

The Federal Trade Commission presented a complaint with the bureau regarding the data mining firm Cambridge Analytica, as well as settlements open to public comment with Cambridge Analytica's former CEO and a software developer who was working with it, contending that they used misleading practices to obtain personally identifiable data of a billion of users of Facebook for voter profiling and targeting.[64]

Facebook has claimed to have no involvement with the third party applications in the previous privacy violations. Facebook claimed that the personal information found with the third parties had been somehow stolen by the third party. This, according to Facebook shifts the fault to the third party applications

Third parties stand to benefit more from the illegal usage of personal information. For most of the third party applications to run effectively and efficiently they would need personal information or data. Some of the third party applications are used in masters of politics which heavily rely on the use of personal information. With the motive to efficiently achieve their goals, third party applications can be blamed for the privacy violations.

[64] https://www.ftc.gov/legal-library/browse/cases-proceedings/182-3107-cambridge-analytica-llc-matter

Facebook has reported and terminated a number of third party applications. This serves to rid Facebook of its allegations and in turn dumps them in third party applications. In another case of privacy violations, When called Facebook stated that its security experts recently alerted the firm to two unlawful actors, One Audience and Mobiburn, who recruited developers to employ malware-filled developer kits (SDKs) in an array of prominent app marketplaces.[65]

"After investigating, we removed the apps from our platform for violating our platform policies and issued cease and desist letters against One Audience and Mobiburn. We plan to notify people whose information we believe was likely shared after they had granted these apps permission to access their profile information like name, email and gender,"this was the statement given by a Facebook representative.

Third party applications are to blame for the privacy violations. The mere existence of third party applications presents itself as a channel to syphon private information or data from social media platforms such as Facebook. If there were no third party applications then, most likely a gap would exist between the private information and the market.

Preventive Measures

As was stated in the first part of this chapter, fault finding without seeking solutions is a waste of time, so this part of this chapter suggests the solutions which can be taken to curb privacy violations.

First and foremost, social media platforms should take care of the user's private information or data and they should actually live to their word of protecting their users. The social media platforms should adhere to the various legislation which have been put to protect the users privacy.

Measures such as those stated under Chapter 2 of GDPR. Which states that several principles have been laid down in pursuit of protection of personal information.

[65] Ibid

Article 5 deals with Principles relating to processing of personal information. It denotes that;-

Personal data shall be following principles

(i) lawfulness, fairness and transparency

(ii) Purpose limitation

(iii) Data minimization

(iv) Accuracy

(v) Storage limitation

For the purposes of this Art, personal data shall be therefore

a) Collected in a legitimate, just, and transparent means for the user.

b) Obtained for specific, explicit, and legitimate reasons, not be processed in ways that contradict those aims further use of such data for archiving reasons in the interests of public, technical or scholarly purposes, or for purposes of statistics shall not be regarded as contradictory with the intended objectives under Article 89(1).

c) Should be sufficient, pertinent, and confined to what is required for the processing purpose.

d) Accurate in addition to whenever required, kept up to date; all feasible efforts must be taken made toward guaranteeing that erroneous individual information, having respect to the purposes for which they are processed, are erased or updated as soon as possible.

e) Maintained in a way that allows the identification of data subjects for no more time than what is required for the purposes for which the particulars are processed; personal data can be retained for longer than necessary as far as the personal data will be processed exclusively for archiving purposes specified in accordance with Article 89(1), subject to the implementation of the appropriate technical and organizational.[66]

[66] GDPR Article 5

Apart from adhering to legislation, the social media platforms should also desist from the practice of drafting predatory terms and conditions. They should make their terms and conditions more humane and allow for enjoyment on their platforms.
They should also cease dealing with third party applications who are interested in private data. If they make it clear that the third party applications siphoning data are not their allies then the war against privacy violations would be a bit easier to tackle.

Users should make efforts to resist giving away their personal information or data. If users can hold onto their personal information it would be a lot harder for their privacy to be violated.

When it is absolutely necessary that the users have to give their information, the users have to be aware enough to read and understand the terms and conditions before they agree to them.
The users should be smart enough to be given full information regarding their personal information that they would have given. They should be able to follow the whole process up to the point where their data is fully destroyed once completion of its usage.

Users have to understand that social media platforms are not only there to protect and ensure data privacy. Users themselves should take tremendous care of their personal information or data.

Users should be smart enough to realize violation patterns and should be able to turn away from suspicious or any social media platform with a record of privacy violations. Users should understand that if a social media platform was able to do it before, it can probably do it again and this time it will take them with it.

Users should hold their personal data up high that they are not willing to trade it for mere social media moments or information.

Third party applications should cease and desist from the action of stealing or illegally obtaining personal information. They should respect the social media platforms and the users and find other ways to collect the data they need which is legal and causes no harm to the users or population at large.

Conclusion

If the current scenario continues, the intersection of the data privacy dilemma and consumer ignorance puts Facebook app developers and comparable companies in an excellent spot to deliberately misuse the personal data of their customers' privacy, despite the regulations designed to safeguard users.

For example, advanced European legislation has called for considerably more transparency regarding the way corporations handle confidential customer data, as well as greater clarity about consent—by offering privacy policies that expressly outline how consumers' data will be utilized and to which users agree.

These rules, however, remain essentially meaningless if users continue apathetic regarding their security and instead just bypass reviewing an app's privacy policy before rapidly agreeing to its terms to begin using the app. Interestingly, such regulations may provide better legal justification for organizations' blatant abuse of users' private data, given how frequently consumers proactively provide the information in question.[67]

There is an inherent need to adopt ways which ensure data protection and security. This would serve in retaining and maintain the positive connotation of social media platforms. This would regain the trust of users which is dwindling away. The revised data protection would also ensure that users enjoy their time on social media.

[67] Ibid

Chapter 5

CHAPTER 5 - PRIVACY AND DATA PROTECTION.

Privacy generally refers to the ability to keep certain aspects of one's life confidential and away from public scrutiny. It involves control over what information to share, how its shared, who has access to the said information and how it is used. Privacy is an important aspect of human dignity and autonomy. It helps protect personal information and allows individual to restrict and control their information in order to safeguard personal liberty and freedom.

Article 21 of the Indian Constitution ensures the right to life and personal liberty. This is a highly important and broad topic, with numerous repercussions for Indian people in general. Article 21 provides for the protection of life and personal liberty, declaring that no one shall be deprived of his life or personal liberty except following the due process of law. [68]The articles ambit was widened to include several rights such as the right to go abroad, right to education and most importantly in modern day, right to privacy.

In his work titled, "The Right to Privacy," Adam Carlyle Breckenridge identifies privacy as a person's liberty to choose how much of himself he wants to reveal to other people, as well as his authority over the conditions, locations, and times under which he communicates with others.[69] He adds that privacy is the right to withdraw or engage as one deems appropriate. It comprises an individual's right to influence the dissemination of information that he owns personally. "The Right to Privacy" was published in 1970 to explore how the Bill of Rights and the Fourteenth Amendment protect persons from unwarranted and unjustifiable interference with their personal privacy.

Privacy individuals to set up barriers and manage boundaries to protect themselves from undue interference allowing them to decide how they want to engage with others. Having privacy enables one to determine how to use their information, who they share their information with, it basically helps individuals better decide the

[68] Article 21: Protection of life and personal liberty - Constitution of India
[69] A.C. Breckenridge, The Rght to Privacy (1971)

who's and who's not of their life. The rules of privacy therefore, allow individuals to assert their rights better when faced with huge power disparities. Today privacy an essential tool for individuals to safeguard themselves and society from arbitrary and unjustifiable use of power, by limiting what can be visible to the public.

Speaking of privacy, it is important to note there would be no privacy issues with data involved. When it comes to information already posted on Facebook or on the public domain, questions as to whether its still entitled to protection or if its still private arise. The Indian courts in R. Rajagopal v. State of T.N held that the publication of information which is already in public domain does not raise an issue of privacy however, if the publication went beyond the public record and reveals one's personal life would amount to invasion of right to privacy.

Modern Day Definition of Privacy

It is without a doubt that the progression of time has changed definitions and understandings of certain concepts, some more than the other. Evolution has seen unprecedented changes which have tipped the balance of many terms. Certain Ideals and values have been shifted from the traditional view to a more modern and befitting understanding. The term, privacy has also been affected by the tides of time.

The traditional view of Privacy was limited to mere non sharing of certain certainties. However, the modern definition has advanced to encompass a wide variety of issues surrounding people, their secrets and their data.

Modern day has coined a variety of concepts ranging from private browsing to privacy curtains.

A new form of privacy, one which is connected to social media, information privacy. This Information privacy is the right to have some control over how your personal information is collected and used.[70]

[70] https://iapp.org/about/what-is-privacy/

With the readily available information on the internet people have begun to learn the real depth of privacy. Over the years, with the popularity of the internet, the society has seen itself in lock horns with the social media platforms for infringement of their private data rights. Initially not much importance was placed in these issues, however, with the expansion of the social media platforms and the increased loss of personal data.

Privacy has extended to include one's personal preferences, be it in terms of foodstuffs to cloth material, but perhaps the most significant range would be extremely personal details such as age, blood type or d.n.a.

Technological advancements have led to more inventions and breakthroughs. However, most of these inventions are targeted to cater for personalized needs. The problem with this now would be presented as a question, how do these organizations make personalized goods and services without accessing personalized information? This is where the wider ambit of privacy plays a crucial role as it covers the said "personalized information".

It has been set in stone that the progression of time and the technological advancements will directly lead to a remolding of the definition of privacy. The more the human race advances the more they realize the true value of personal information and the need to protect it. Thus, despite modern day privacy stretching to include both the physical realm to the online realm it is far from reaching its final form.

Data Privacy

Data privacy is a crucial aspect of any organization that handles personal information of customers, employees, or other stakeholders. However, data privacy is not a one-size-fits-all function, and different roles may have different scopes and responsibilities depending on the context, goals, and challenges of the data privacy program.[71]

[71] https://www.linkedin.com/advice/0/how-do-you-define-scope-responsibilities-data-privacy?src=go-pa&trk=sem-ga_campid.20316911727_asid.154319842041_crid.663989285742_kw._d.m_tid.dsa-2089354983777_n.g_mt._geo.9061682&mcid=7080236969011671041&cid=&gad_source=1&gbraid=0AAAADpfA-0zX7F_sXxpAaccxogKdolUp&gclid=CjwKCAjwgdayBhBQEiwAXhMxtjM09u4KJY3O-2b42mX0tON4RvZtCTNpn-ml6hmHAPNNWMCaHO_sghoCjO8QAvD_BwE&gclsrc=aw.ds

Data privacy alludes to a person's ability to choose the manner in which and to the degree that their personal information is shared with or disclosed to third parties. This personal information may include their name, place of residence, contact details, or digital or real-life practical conduct.[72]

As the use of the internet has grown over time, so has the necessity of data privacy. Websites, software, and social media platforms frequently gather and retain the personal information of users to provide services. However, some programs and platforms might go beyond users' expectations for data gathering and utilization, resulting in less privacy than they anticipated. Other software applications and networks may not put proper controls on the data they gather, resulting in a breach of security that infringes user privacy.[73]

The importance of data privacy

Data privacy, much like any other form of privacy is of very high importance as it guarantees boundaries and their recognition. Privacy, in various jurisdictions, is recognized as a fundamental human right, and several data protection laws exist to guard that right.

Data privacy is also of paramount importance as it allows the users to engage with each other with the assurance that their information stays classified. Which is why most platforms on the internet advertise their platforms by highlighting how they took care of data privacy, for example most of the social media apps, especially dating apps.

Principles of Data Privacy

In many firms, data privacy is handled by a multidisciplinary staff that includes legal, adherence, IT, and cybersecurity experts. These departments create data management policies that regulate how their firms gather, utilize, and secure personal data while

[72] https://www.cloudflare.com/en-in/learning/privacy/what-is-data-privacy/
[73] Ibid

respecting consumer confidentiality expectations. They additionally develop methods for users to assert their rights and establish technical measures to protect data.[74]

The principles are as follows;-

1. Access;- this guarantees that those who opt to provide personal information or data should have access to the data or information that they give. No corporation or body corporate should restrain anyone who gives his personal information to access that personal information or data.
2. Transparency;- information regarding the personal information or data, such as which other organizations have access to it and how it's being transferred, should be given to the users who would have given their personal information or data.
3. Consent;- the users who opt to give their personal information should expressly do so in a non misrepresented manner. The users should freely give their express consent for any storage, sharing or processing of their personal information.
4. Quality;- the personal information gathered should be of high quality, that is accurately. The best quality of any information is seen by its accuracy.
5. Security;- organizations and platforms should put in place effective security to watch over the priceless personal information or data.

Data Protection and Privacy

The concepts of data protection and data privacy are frequently used in tandem, but there exists a key distinction between the two. Data privacy determines who has access to data, whereas data protection provides means and rules to limit access to data. Compliance requirements aid in ensuring that corporations carry out user privacy inquiries, and they are accountable for taking precautions to secure private user data.[75]

[74] https://www.ibm.com/topics/data-privacy
[75] https://cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data

Data privacy and data security are two separate but linked fields. Both are integral parts of a company's overall information management strategy.

Imagine a website obtains personal information from clients in the European Union during the course of their transactions. The personal data contains specific details which include the client's name, place of residence, and phone number. For all, the goods must be sent to the client in Europe. The website's operator stores and ships merchandise through an external warehouse, a third party. To ensure that the packages arrive at their intended destination, the website operator shares the client's name along with their address with the warehouse. The warehouse then ships a box containing the ordered merchandise to the customer. The "controller" in this case is the one who operates the website as they obtain data and decide the way it is handled. The warehouse would be the processor. This a very a good example of data processing , controlling and third party transfer.

Data Protection

Data protection is most probably the key to achieving privacy in modern day settings. It is the guide to achieving privacy in its advanced current state. Data protection is the safeguarding of sensitive information from loss, corruption or damage. Failure to which will result in financial losses, loss of reputation and customer trust, and legal liability. The danger it carries makes it perhaps the most significant impediment to digital transition in enterprises of all kinds, as well as people. As a result, most methods for protecting data focus on three critical areas: Data security - the protection of data against deliberate or unintentional harm. Which raises the question of whether you are who you claim to be. Data Availability - ensures efficient data storage in case of damage or loss. This guarantees that the data is easily accessible for utilization. Access control - ensures data is only accessible to authorized users.

Principles of Data Protection

Article 5 of the General Data Protection Regulation (GDPR) establishes key concepts that serve as the driving force of the general data protection regime.

In a wider sense the principles denote that personal information shall be dealt with accordingly with;

a. Lawfulness, fairness and transparency;- indicating that, when dealing with personal data, it shall be done so in a legal manner which shall also be executed via good governance measures.

b. Purpose limitation;- this dictates that personal information shall be dealt with in such a way that it's use will be limited to that which it was collected for and further processing will be prohibited.

c. Data minimization;- this states that personal information or data should not be collected in abundance. Only required data to be given, nothing more.

d. Accuracy;- This requires that the personal information must be accurate, and in case it isn't, swift action should be taken to rectify the same.

e. Storage limitation;- this dictates that the limitation period of storing personal information should be adhered to.

f. Integrity and confidentiality;- this denotes that the personal information should be thoroughly protected against loss, damage, destruction or theft.

g. Accountability;- the responsible parties in possession of the private information shall take responsibility of the data at all times.

Data controllers are accountable for adhering to the principles and language of the legislation. Data controllers are likewise held accountable for how they handle it and must show compliance. This is specified in the new accountability concept.[76]

Privacy As A Right.

Chief Justice J.S khehar stated that, "privacy is intrinsic to the right of life and personal liberty under Article 21 of the Constitution and will be included under part 3 of the Constitution.". [77]

The Supreme Court in R. Rajagopal v. State of Tamil Nadu [78]held that the right to privacy or the right to be let alone is implicit in the right to life and liberty guaranteed under Article 21 of the Indian constitution. The court in this case noted two components of the right to privacy:

(i) The tortious law of privacy which grants an action for damages resulting from an unlawful invasion of one's privacy and,

(ii) The constitutional right to be let alone implicit to the right to life and personal liberty under Art 21.

While the court recognized one's right to safeguard and protect his privacy, it also acknowledged exceptions to this rule. It stated that where the issue has become a matter of public record, the right to privacy can not be claimed and public officials are not entitled to claim privacy when the act in question relates to discharge of their official duties.

The case laid down several principles on the same and these include the following just to name a few:

(i) No one shall publish anything concerning a person's private concerns without their consent whether true or otherwise, laudatory or critical;

---

[76] https://www.uhi.ac.uk/en/about-uhi/governance/policies-and-regulations/data-protection/the-seven-principles/

[77] Priyanka Mittal, Right to Privacy: What Supreme Court judges said in separate judgments, (Original -25 Aug 2017), Available At: https//www.livemint.com/Politics/RzzefgmBSSNrWODUJklGEP/Privacy-as-a-fundamental-right-What-Supreme-Court-judges-sa.html.

[78] 1995 AIR 264, 1994 SCC (6) 632

(ii) The position will be different if a person voluntarily thrusts himself into controversy;

(iii) Certain public records may not be published in the interest of decency

(iv) Publication based upon public records is permissible even if it violates the right to privacy[79].

The Right to be Forgotten

The right to be forgotten, also known as the right to erasure, is a civil right that allows individuals to have their personal information deleted from the internet. This concept entails the right of an individual to have information about them removed and erased to the extent that it is eventually forgotten by the public. A traceable system must be in place to verify that removed data is purged from backup storage media. It simply stipulates that everyone has a legal right to have their information removed and erased from public eye in the internet. This right was recognized in the Google case of Google Spain LS, Google Inc. V. Agencia Española de Protección de Datos, Mario Costeja González (2014), where the Court of Justice of the EU granted the right to individuals to request search engines like Google to remove links containing information about them. [80]

The concept of right to be forgotten was first known as an extension of right to privacy. In another landmark case of Gabrielle Darley Melvin v. Dorothy Davenport Reid,[81] the Court of Appeal of California held that the release of a picture depicting the life of a former sex worker who had been entirely reformed and was leading an honorable life, was an act of unlawful invasion of her right to privacy guaranteed under the constitution.

Domestically, in India, the right to be forgotten has not been fully recognized under the law. While there is no formal legislation that lays down this right, the Courts have on their own recognized this right as part and parcel to the right of privacy subject to certain limitations. The right to be forgotten was first practiced against the medianana.com website which was requested to remove a link.

[79] 1995 AIR 264, 1994 SCC (6) 632
[80] EUR-Lex - 62017CJ0507 - EN - EUR-Lex (europa.eu)
[81] Melvin v. Reid, 112 Cal.App. 285, 297 P. 91 (Cal. Ct. App. 1931)

Sri Vasunathan v/s The Registrar General & Ors., the single bench court held that although there exists no statute that conferred the right, in the wake of the increasing importance being placed on an individual's right to privacy and the adoption of rules dealing with right to be forgotten in foreign jurisdictions like Europe, it would only be in the right interest of justice to pave way for the same in India[82].

In V. v. High Court of Karnataka, the Karnataka High Court recognized right to be forgotten[83]. The court in this particular instance stated that its verdict was in line with the pattern observed in Western countries, wherein the 'right to be forgotten' has been used as standard procedure in delicate situations involving women in general, along with particularly sensitive scenarios that involve sexual assault or affecting someone's self-respect and image.

It is to be noticed that currently the right to be forgotten has been perceived as a basic face of the right to privacy. The Government in 2019, launched the Personal Data Protection Bill, which focused on regulating data processing by both government and non-government companies. Article 20 of this measure dealt solely with the right to be forgotten, its implementation, control, and restriction. It mandated the enforcement of the right only through the sanctioning by a concerned Adjudicating officer, and it also carved out provisions for review and appeal of such Adjudicating officer's orders.

Privacy and Free Speech

The right to privacy has been regarded with the right to freedom of speech. It is important to note that these two are two sides of the same coin and this is because one’s right to free speech and expression, to be informed and know might violate another’s right to privacy- right to be left alone. Now, while freedom of speech is an important part of disseminating information, it is equally important to protect the private life of an individual even in cases of public interest.

[82] Vasunathan v. Registrar General | Karnataka High Court | Judgment | Law | CaseMine
[83] https://www.scconline.com/blog/post/2022/01/27/the-evolution-of-right-to-be-forgotten-in-india/

Legislative Framework.

Despite the rampant abuse of the right to privacy, several laws exist to protect the privacy of internet users. Several legislation's have been drafted to secure private data on the internet. However, there hasn't been no one enactment which comprehensively governs data protection in India, the legal provisions governing the same need to be derived from various legislative enactments.

General Data Protection Regulations (EU) 2016/679

This legislation came into power in 2018 with the objective of protection of personal information. This legislation, despite being bound to the EU serves as an important source for legislation in other countries.

Under **Chapter 2** several principles have been laid down in pursuit of protection of personal information.

Article 5 deals with Principles relating to processing of personal information.

For the purposes of this Art, personal data shall be therefore

a) Collected in a legitimate, just, and transparent means for the user.

b) Obtained for specific, explicit, and legitimate reasons, not be processed in ways that contradict those aims further use of such data for archiving reasons in the interests of public, technical or scholarly purposes, or for purposes of statistics shall not be regarded as contradictory with the intended objectives under Article 89(1).

c) Should be sufficient, pertinent, and confined to what is required for the processing purpose.

d) Accurate in addition to whenever required, kept up to date; all feasible efforts must be made toward guaranteeing that erroneous individual information, having respect to the purposes for which they are processed, are erased or updated as soon

as possible.

e) Maintained in a way that allows the identification of data subjects for no more time than what is required for the purposes for which the particulars are processed; personal data can be retained for longer than necessary as far as the personal data will be processed exclusively for archiving purposes specified in accordance with Article 89(1), subject to the implementation of the appropriate technical and organizational.,[84]

f) processed in a way that provides adequate safety of personal data, including safeguards against unlawful or unauthorized access as well as unintentional theft, deletion, or destruction, using suitable technical or organizational methods.[85]

Article 6 – deals with Lawfulness of processing personal information.[86] According to the article, processing is lawful if and only if at least one of the following conditions is met:

a) The data subject has granted authorization to the handling of their private information for one or more defined purposes.

b) Processing is required for the execution of a contract in which the data subject is a party, or to perform actions at the user's request before signing a contract.

c) Processing is required to comply with some certain legal obligation.

d) Processing is essential to safeguard the fundamental interests of the data subject or another natural person.

e) Processing is required for executing an action in the public interest or official authority.

f) Processing is required for legitimate interests pursued by the controller or a third party unless bypassed by the data subject's basic liberties and freedoms that

[84] https://gdpr-info.eu/art-5-gdpr/
[85] Ibid
[86] https://gdpr-info.eu/art-6-gdpr/

necessitate personal data protection especially when the subject in question is a child.

Article 9 – deals with the processing of special categories of data.

Article 10 – deals with the processing of data relating to criminal convictions and offences

Chapter 3 of the GDPR, deals with Rights of the data subject.

Article 12 – relates to transparent information, communication and modalities for the exercise of the rights of the data subjects. It states that;-

a. The controller must provide information and communication about the processing to recipients of data in a comprehensible language, especially for children, as per Articles 13-14 and 15-22 and 34. The information must be delivered through writing or via other methods, which include, where necessary, electronic means. Whenever desired by the data subject, the information may be provided orally, granted that the recipient's identification is established by any other method.

b. The controller must enable the enjoyment of the rights granted to data subjects under Articles 15 to 22. 2In the instances alluded to in Article 11(2), the controller must decline to act on the data client's request to exercise their rights under Articles 15 to 22, except the controller establishes that it has no way of correctly identifying the data subject.

Article 13 – denotes the information which is supposed to be provided where personal data is collected from the data subject. It states that;-

Whenever personal data is gathered from a data subject, the controller must furnish the following information to the data subject;-

(a) Controller and representative contact information

(b) Data protection officer contact information

(c) Personal data processing purposes and legal basis

(d) If processing bases itself on clause (f) of Article 6(1), the legitimate interests sought by the controller in question or an outside party, and

(e) the subjects or classes of users of the personal data, if applicable.

(f) where necessary, the fact that the controller is planning on transferring personal data to a different nation or global organization, and the presence or lack of an adequate decision by the Commission, or in the event of transfers mentioned in Article 46 or 47, or the subsequent clause of Article 49(1), the allusion to the necessary or appropriate security measures and how to get a duplicate of such data or where they have been rendered accessible**.**

Article 14 – deals with information to be provided where personal information has not been collected from the data subject.

Article 15 – is in regards to right of access of the data subject. It denotes that;-

The data subject has the right to receive assurance from the controller as to whether or not personal data concerning them is being stored, and, if it is the case, have access to any such data and the additional details that follow:-

a. Objective of processing,

b. Types of personal data involved.

c. The users or groups of users to whom the specific information has been transferred or will be provided, particularly users in other nations or worldwide organizations.

d. Where feasible, the intended time for which the private information will be held, or, in the absence of possible, the standards used to calculate the time frame in question,

e. The right to request correction, removal, or constraints of personal data processing, as well as the right to file a grievance with a supervisory authority.

f. In the event the personal data was not obtained from the data subject, any available details about the source of information.

g. The implementation of automated procedures, particularly profiling, which is referenced in Article 22(1) and (4), and, at least in those situations, significant details regarding the reasoning at play, as well as the relevance and the anticipated implications associated with such processing for the data subject.[87]

Article 16 – deals with right to rectification

Article 17 – denotes the right to erasure (right to be forgotten)

Article 18 – deals with the right to restriction of possessing. It states that:-

The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

(a) The data subject contests the accuracy of the personal data, allowing the controller to confirm it.

(b) The processing is unjust and the data subject disagrees with removal, requesting limitations of use instead.

(c) The controller no longer requires the personal data for processing purposes, but the data subject requires it for the establishment, exercise, or defence of legal claims.

[87] Ibid

(d) The data subject expressed opposition against processing under Article 21(1), awaiting confirmation of whether the controller's legal grounds outweigh those of the data subject. [88]

Information and Technology Act 2000 and Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules 2011

The IT Act has been considerably effective in achieving its objectives, especially with its 2008 amendments which equipped the Act with multiple provisions catering to data protection, penalties and compulsory privacy policies.

Relevant provisions, in regards to Privacy, of the Act;

- **Section 43a, b, and i-** It states that any person, who without the permission of the owner, or any other person who may be in charge of a computer, computer system or computer network – It states that any person, who without the permission of the owner, or any other person who may be in charge of a computer, computer system or computer network –

a) Gains access to any computer, system, or network.

b) Downloads, copies, or extracts data from a computer, system, or network, including information saved on a removable storage drive.

c) The person who steals, hides, destroys, or modifies any computer source code that is utilized for the purposes of computing with the intent to cause harm will be held accountable to pay damages by way of compensation up to the sum of INR 1,00,00,000 (rupees one crore) to the aggrieved person.

- **Section 43a** is the foundation of data protection. It states that if a company negligently handles sensitive personal data on its computer resources and causes wrongful loss or gain, it will be held liable for damages and compensation.

- Under **Section 66c**, anyone who falsely or dishonestly uses another person's

[88] Ibid

electronic signature, password, or other unique identification feature may face imprisonment for up to three years.

- **Section 72 –** stipulates that any person who gains access to any computerized document, work, register, correspondence, information, document, or other material without the authorization of the person concerned and following that reveals such information to any other person shall be punished with imprisonment for a term that may extend to two years, or with a fine of up to INR 1,00,000 (rupees one lakh),or both.[89]
- **Section 72a -**provides that, anyone, including a third party, who, while rendering services according to the provisions of a lawful contract, obtains access to any material with personal information about someone else, intending to cause or know that he is probably going to cause wrongful loss or wrongful gain, reveals such information to any other person, without the approval of the person concerned, or in violation of a lawful contract, shall be punished with imprisonment for a term which may extend up to three years, or with a fine which may extend up to INR5, 00,000 (rupees five lakh), or with both[90]

The IT Rules require body corporates that store sensitive personal information about users to follow specific security standards Listed below are some of the most relevant Provisions of the IT rules:

Rule 4 – dictates that corporate bodies or any person who on behalf of body corporate, collects, receives, possesses, stores, deals or handles information of provider of information should provide for a privacy policy for handling of or dealing in personal information including sensitive personal information or data and ensure that the same are available for view by such providers of information who have provided such information who have provided such information under lawful

[89] IT Act 2000
[90] Ibid

contract. The policy must be displayed on the website of the corporation in question or any person acting on its account.

a) It should include explicit statements of practice and policies,

b) Type of personal or sensitive information gathered under rule 3.

c) Objective for gathering and using information;

d) Distribution of vulnerable identifiable data as per rule 6;

e) Adherence to appropriate security regulations and protocols as outlined in rule 8.[91]

- **Rule 5 –** provides the procedure to be followed for the collection of information by the body corporate or any person on its behalf. Specifies the mechanism for collecting information by the corporate entity or its representatives.

a. Before collecting sensitive personal data or information, the provider must provide written consent in the form of a letter, fax, or email describing the purpose of use.

b. The body corporate or any person acting on its behalf is prohibited from gathering sensitive personally identifiable information unless the information is gathered for legitimate reasons related to the work or operations of the body corporate or any person acting on its behalf, and that it is deemed necessary to accomplish that purpose.

c. While accumulating data directly from the concerned individual, the body corporate or any person acting on its behalf must employ any measures that are reasonable in the context to make sure that the individual in question has enough knowledge that the information is being gathered; the objective why the data is being collected; the intended beneficiaries of the information; and the full name and address of the entity responsible for obtaining the same.

[91] Information Technology Rules 2011

d. Furthermore, the body corporate or any person acting on its behalf retaining sensitive personal data or information is prohibited from keeping such data for a longer period than is necessary for the reason for which the data may be legitimately utilized or as prescribed by any other law currently in effect. The data that was collected can only be utilized for the exact reason for which it was acquired.

e. The body corporate or any person acting on its behalf shall allow the information providers to scrutinize the data they gave whenever requested, and make sure each piece of sensitive personal data, or information discovered to be incorrect or inadequate is rectified or modified as soon as possible. However, a body corporate can not be held accountable for the accuracy of personal information, sensitive personal data, or information provided by the information source to the body corporate or any other person working on its behalf.

f. Before collecting information, including sensitive personal data or information, the body corporate or any person acting on its behalf must give the information provider the chance of not providing the data or information intended to be acquired. The information provider should have the opportunity to terminate its previously granted approval to the body corporate at any point, whether using the services or otherwise. Such a withdrawal of permission must be communicated in writing to the corporation. If the information source fails to grant or later withdraws its consent, the body corporate may refuse to deliver the goods or services for which the information was requested.

Rule 6 – deals with the disclosure of information by body corporate to any third party.

a) It states that disclosure of sensitive personal information or data by a body corporate to any third party requires advance authorization from the provider of such information, who has provided such information under a lawful contract or otherwise unless the sharing was agreed upon in the contract between the body corporate and the provider of information, or where the disclosure is required to comply with a statutory requirement. Yet, without the provider's express

permission, the information provided must be shared with authorities ordered by law to obtain information, including sensitive personal data or information, for identity verification or prevention, detection, and investigation, including cyber-related events, legal action, and penalty of offences. Government bodies must submit a written request to the corporate entity in possession of sensitive personal data or information, explicitly indicating the objective for requesting such information. The requesting agency must additionally clarify that the information received will not be disclosed or disclosed to anybody else.

b) Notwithstanding anything in such Rule, any sensitive personal information or data may be released to any other party according to an order issued under the legislation in effect at the time.

c) The body corporate or anybody acting on its behalf may not disseminate sensitive personal data or information.

d) A third party obtaining sensitive personal information or data from a corporate entity or any person acting on its behalf is not permitted to divulge it further.

Rule 8 – the corporate body is required to, while handling personal information or sensitive personal information or data, comply with reasonable security practices and procedures.

a) A body corporate or a person acting on its behalf is deemed to have adhered to adequate safeguards and processes when they have implemented these safety precautions and requirements, as well as an extensive documented information security program and information privacy regulations that include managerial, technical, functional, and operational safety procedures corresponding with the nature of the business and the information resources that are being protected.

b) In the event of a data security violation, the body corporate or a person on its

behalf is obligated to prove, should they be asked upon to do so by the agency authorized by the legislation, that they have adopted security control measures as documented information security programs and policies. The International Standard IS/ISO/IEC 27001 on "Information technology – Security Techniques – Information Security Management System – Requirements" is one such standard which must be adhered to.

c) Any industry cooperation or entity established by such an association whose members self-regulate by adhering to codes of best practices other than IS/ISO/IEC for data protection must have its codes of best practices approved and notified by the government of India for efficient execution.

d) The body corporate or person acting on its behalf who adopted either the IS/ISO/IEC 27001 standard or the codes of best practices for data protection is considered to have adhered to reasonable security practices and procedures if those standards or codes of best practices have been registered or reviewed regularly by entities through independent auditors approved by the Central Government. An auditor must audit reasonable security measures and procedures at least annually, or whenever the body corporate or a person acting on its behalf makes major upgrades to its processes and computer resources.

The Aadhaar (Targeted Delivery of Financial and other Subsidies Benefits and Services) Act 2016

Section 28, of the Act states that:- (1) The Authority shall safeguard the security of persons' identity information and authentication records.[92]

2) Based on the terms of this Act, the Authority shall safeguard the

[92] The Aadhar Act 2016, section 28

confidentiality of persons' identity information and authentication records.

3) The Authority shall implement all necessary measures to guarantee that the information in its custody or control, including information stored in the Central Identities Data Repository, is adequately safeguarded against access to it, usage, or leakage that is unlawful under this Act or its regulations, as well as accidental or deliberate harm, loss, or damage.[93]

4)Without prejudice to sub-sections (1) and (2), the Authority shall—

a) Introduce and employ suitable relevant and organizational security measures.

b) Guarantee that agencies, consultants, advisors, or other individuals designated to perform any function of the Authority under this Act have necessary technical and organizational security measures in set for the information.

c) Ensure that any contracts or arrangements formed with such agencies, consultants, advisors, or other persons impose duties akin to those imposed on the Authority under this Act, and necessitate such agencies, consultants, advisors, and other persons to act only on the Authority's instructions.[94]

(5) Notwithstanding anything mentioned in any other law currently in effect, and except as explicitly stated in this Act, the Authority or any of its officers or other employees, or any agency that maintains the Central Identities Data Repository, are forbidden to disclose anything maintained in the Central Identities Data Repository or confirmation record to anyone, whether throughout his tenure or thereafter.[95]

Provided that an Aadhaar number holder may request that the Authority grant access to his identification information, excluding his core biometric information, in

[93] The Aadhaar Act 2026, section 28(3)
[94] Ibid
[95] Ibid

the manner provided by rules.

Section 29. states that (1) No core biometric information, collected or created under this Act, shall be—

(a) shared with anyone for any reason whatsoever; or

(b) used for any purpose other than generation of Aadhaar numbers and authentication under this Act.[96]

(2) The identity information, other than core biometric information, collected or created under this Act may be shared only in accordance with the provisions of this Act and in such manner as may be specified by regulations.[97]

(3) No identity information available with a requesting entity shall be—

(a) used for any purpose, other than that specified to the individual at the time of submitting any identity information for authentication; or[98]

(b) disclosed further, except with the prior consent of the individual to whom such information relates.

The Legitimacy of Personal Data Protection Bill (2019)

The Ministry of Electronics and Information Technology introduced The Personal Data Protection Bill in the Lok Sabha in 2019. This bill was largely based on the GDPR.

The bill defined "personal data" under section 3, as, data about or relating to a natural person who is directly or indirectly identifiable, having any regard to any characteristic, trait, attributes or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any

[96] The Aadhaar Act 2016, section 29
[97] Ibid
[98] Ibid

other information, and shall include inference drawn from such data for the purpose of profiling.[99]

The bill also gives grounds of processing of personal data. Section 15(1) of the Personal Data Protection Bill (2019). Similarly to the GDPR, the Personal Data Protection Bill, also deals with the right today's erasure. It deals with this right under section 18.

The amendments to the act introduced new recognized categories of data fiduciaries and these categories were Consent Managers and Social media intermediaries.

Social media intermediaries have been defined under section 26(4) of the Personal Data Protection Bill 2019. They were defined as "an intermediary who 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 intermediaries which primarily;

(a) Enable commercial or business oriented transactions,

(b) Provide access to the internet,

(c) In the nature of search engines, online encyclopedias, email services or online storage services." [100]

Right to Information Act

While most of its sections, grant access to information, the RTI Act has several sections which imposes exceptions to disclosure of information.

- Section 8(1)(j) – stipulates that the authorities are not obligated to furnish information to citizens concerning inter alia, information relating to personal information, the disclosure of which has no relevance to any public activity or interest, or which would result in an unlawful invasion

[99] Section 3 (28) of the Personal Data Protection Bill 2019
[100] Section 26 (4) of the Personal Data Protection Bill 2019

of the one's privacy, unless the Central Public Information Officer, the State Public Information Officer, or the appellate authority, as the case may be, is satisfied that the disclosure of such data is justified as it is of public interest. Provided that the information that cannot be refused to the Parliament or a State legislature will not be withheld to any person..[101]

[101] Right to information Act section 8

CHAPTER 6

CHAPTER 6- CONCLUSION AND SUGGESTIONS.

In 2005, while social media was still in its early life, only approximately 5% of US users engaged actively on it. In 2019, that figure increased to almost 70%. The internet world continues to grow rapidly and as more opportunities are presented, more challenges are also evoked. The same with any other legislation and rules, the internet sphere should have ever-evolving laws which will ensure that neither the users nor the corporations are taken illegal advantage of. With so much data on user social media accounts, criminals can gather ample information to track users, assume identities, and try schemes. Data protection concerns and vulnerabilities in privacy measures might place user information in danger when using platforms such as Facebook.

The research strives to understand the privacy and privacy violations on social media platforms. It was narrowed down to focus on identifying the criminal and civil liabilities of Facebook in privacy violation issues. The most critical questions for this research were as follows:

1. Who is liable for privacy violations committed on Facebook?
2. Do users comprehend the consequences of their consent when accepting the terms and conditions?
3. Why are there concerns surrounding privacy on social media?
4. What does social media do to protect users' privacy and data?

These questions were addressed directly and directly concerning Facebook. The issue of liability was found to be one arising from both parties. The users, be it the new carefree latest generation, do not take adequate time to understand the terms and conditions. The younger generation, and even the older generation, tend to blindly agree to the terms and conditions without even reading them. This would lead to future unwarranted “violations”.

However, not to say that the social media platforms, Facebook in particular, are doing due diligence in protecting and storing the user's data. In many instances,

Facebook blatantly ignores restrictions and regulations relating to users' privacy. Most of the unraveled cases against Facebook show that indeed it had not taken adequate care or it was grossly negligent in performing its duties.

The research also proved that comprehension of terms and conditions was far from being achieved by the users. An estimated one in twenty-five people have outlined that they “know and have seen” where the terms and conditions are on the social media platforms. However, the number dropped drastically when they were asked whether or not they read and understood the terms and conditions.

Attributing to the numerous cases of privacy violations by social media platforms, Facebook, it is warranted that there would be raised concerns regarding privacy and social media platforms. In present times, not a year passes without new cases of violations of privacy on social media platforms.

These numerous cases have uncovered the horror of how social media platforms store users' information. In some of the cases, the social media platforms would plead no relation to third-party applications that would have acquired personal information. This shows the gross negligence on the part of the social media platforms in safekeeping the personal information or data of the users.

The whole research was executed through the use of various literature. It was astonishing to realize, despite how little was known in the earlier days of the internet, that concerns had already been made regarding privacy on the internet. It is disheartening to read through the cases against social media as they only show how less effective the regulations are in dealing with the social media platforms' wrongdoings. Most of the fines are of very little or no effect on high-earning social media platforms. The lack of effective punishment is simply outrageous.

Future Recommendations

Future works related to the topic of this thesis would be very useful in both raising awareness and reminding the legislators of their duty to realize the people’s rights. For future works, it would be effective if more focus is drawn to the legislators and

other law enforcement agencies who are letting these social media platforms run rampant with people's private information.

Future studies should highlight how the proposed suffering due to the violations in privacy and data storage of users.

User education and awareness should be raised. Future literature and media works should emphasize teaching the user the importance of safeguarding their private information or data. If awareness is raised, less blind consents and agreements to predatory terms and conditions will be made thereby restoring privacy one user at a time.

Studies and research on third-party applications' roles in privacy violations should also be made popular to raise awareness all around.

Contribution to the field

This study has shed light on how the users are ignorant of the terms and conditions and how it affects them in the long run. It has also shown how social media platforms are setting up unjust and unfair terms and conditions which are preying on the private information of the users. The study has also highlighted how the legislation and the rules are lagging.

In conclusion, privacy violations on social media are attributed to three major players, the user, the social media platform and the third parties. Each party has been playing its part relentlessly. The only way to reduce the privacy violations would be to address all the parties individually.

The users need to be educated and made aware enough to recognize predatory terms and conditions. The users should be reluctant to give away their private information or data. They should inquire about the procedure in which their data will be used in.

Social media platforms, Facebook in particular, should recognize their size and strive to positively impact society. The social media platforms should devote themselves to protecting the user's information which they would be entrusted with.

They should also adhere to the rules and regulations and keep their business and transactions transparent

Third-party applications should refocus their attention from stealing and unlawfully benefiting from the user's private information.

BIBLIOGRAPHY

- *Law and Media* – Dr Rattan Singh, Dr Shruti Bedi
- *Cyber law; Law of Information Technology and Internet* – Anirudh Rastogi
- *Facets of Media law* – Madhavi Goradia Divan (Second Edition)
- *Media Law; India and Abroad* – Purvee Malpani