Library Progress International
Vol.44 No. 3, Jul-Dec 2024: P. 15638-15644

Print version ISSN 0970 1052
Online version ISSN 2320 317X

Original Article

Available online at www.bpasjournals.com

Personal Data on Social Media: Threat to Privacy Right

[1]Dr Sharafat Ali, [2]Dr Archana Sharma, [3]Prof (Dr) Jageshwar Nath Singh, [4]Dr Gireesh Kumar Kapil

[1] Siddhartha Law College, Dehradun Uttarakhand (India)
[2]Principal, BSM Law College, Roorkee, Uttarakhand (India)
[3] College of Legal Studies, COER University, Roorkee Uttarakhand (India)
[4] Principal, Chaman LaL Law College, Landhaura Uttarakhand (India)

How to cite this article: Sharafat Ali, Archana Sharma, Jageshwar Nath Singh, Gireesh Kumar Kapil (2024) Personal Data on Social Media: Threat to Privacy Right. *Library Progress International,* 44(3), 15638-15644

ABSTRACT

The definition of privacy is succinctly delineated as the space where one can speculate on his thoughts and ideas without intrusion from others. Being free from prying eyes, interference with one's deeds or beliefs, or intense oversight has been well-described as having privacy. Article 21 of the Constitution of India, addresses the rights relating to one's life and individual liberty and covers the right to privacy. According to this article, everyone has a right to personal space as well as the absolute freedom to live their lives in dignity.

Social media in all of its incarnations, has taken over the internet. It enables one to publicly acknowledge their opinions and thoughts with a multitude of individuals at once. With the proliferation of smart gadgets and universal connections, social media use has grown in popularity. The risk of exposed sensitive data given by consumers does exist, nevertheless. It's feasible that users occasionally aren't aware that the platforms are gathering and sharing their information with other users. These platforms guarantee that users' privacy is protected by assuring them of their privacy policy, as data harvesting is currently at the forefront of technology. But the truth is, users' personal information stored on platforms that, don't ensure effective security, is vulnerable to hacking and data leakage. There has been considerable thought put into whether or not these social media networks protect our privacy. The goal of this study is to define the idea of privacy in the current cybernetic era. Concerns about the world's youth are raised by the question of whether media platforms uphold privacy rights. Many naively believe the hyped-up claims and promises made by these platforms, but in fact, they fall short of giving us the proper data protection. So far, it is ultimately the user's duty to secure personal data. It is essential that we are cognizant of the hazards and take precautions to secure our personal information.[1]

Keywords: *privacy, social media, data protection, right to life*

Introduction

Privacy is one such concept that is acknowledged by all facets of human civilization. It is a broad idea that is widely acknowledged. In a more confined meaning, it refers to having intellectual autonomy and authority over one's beliefs. To protect their personal information and activities from prying eyes, outside observers, or intrusive interference, people ought to be able to regulate their details and behaviour. Privacy can be seen as a basic human right that is necessary for a person's autonomy, dignity, and uniqueness.

In today's digital era, where a significant amount of the personal information we disclose online and offline is gathered, analyzed, and used by numerous entities, including governments, businesses, and people, privacy has become more and more crucial. This raises questions regarding the possible abuse of an individuals sensitive information and the invasion of their privacy rights.

The Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights both include the right to private life as one of the absolute freedoms guaranteed by them. Practically speaking, the right to privacy can encompass things like the liberation to choose one's religion, the right to govern one's digital data, the right to keep personal information private, and the freedom from unauthorized searches of one's home or personal life.

Law Perception and Privacy

1

The idea of privacy has been the subject of numerous knowledgeable philosophers' thoughts and opinions; they have affirmed it as an intrinsic right and declared that everyone must be rightfully able to have their domain where they may utilize their private space without interference from others.

The notion of privacy was articulated by American philosopher and social scientist Alan Westin in the 20th century. According to him, maintaining one's privacy is essential for preserving one's freedom and authority over one's personal information. Westin put up a privacy paradigm with four guiding principles: isolation, proximity, obscurity, and reserve.[2] In order to regulate how much of our personal information we divulge to others, he redefined privacy as the capacity to do so.

Another American philosopher who addressed the idea of privacy was **Shoshana Zuboff**. She wrote prolifically on how global internet giants persuade us to give them our data in her book "The Age of Surveillance Capitalism,". She detailed how these corporations are gathering our data on a worldwide scale and sharing it with others by deceiving people. She claimed that this practice poses a danger to our privacy and independence.

Louis Brandeis was an American jurist who published a legal article review in which he asserted that every individual is born with and possesses the right to privacy, regardless of race or place of birth. Brandeis thought that privacy was crucial for people to form their own identities and that it served as a vital check on the power of the state and corporations. A closer look at the idea of one's right to privacy is necessitated by current developments and the advancing age of commercial engagements. The erosion of privacy has resulted from the rapid dissemination of photos and news stories showing a peek into someone's personal area.[3]

Friedrich Nietzsche also expressed his views on privacy. In his book **"Beyond Good and Evil**," he said that individuality, which includes privacy, is one factor that keeps individuals from interacting with one another in a group. He argued for a more communal way of life because he thought that seclusion served as a barrier to genuine human connection. He believed that in order to resist the unsettling impact of society, there should be a feeling of solidarity.

Nowadays, the growing link between people and organizations poses a risk to people's privacy. When one interacts socially with another person or entity, they reveal personal information that is at risk of being exploited by these so-called protective groups. The essential values of trust are the foundation of this connection. In every contractual arrangement, it is anticipated that the disclosed information will be utilized honestly and securely.[4]

In 2015, the Human Rights Council established a mandate by evaluating government actions and strategies, adopting best practices to allow privacy protection, respecting human rights, and taking particular efforts to explain the laws and processes establishing person's private rights, it enabled the special rapporteur to preserve individual privacy.[5]

Right to Privacy and Judicial Verdict

Privacy rights are not initially assured by the constitution, rather, it is only protected by Article 21 of the Constitution of India. The protection ensuring solitude in all of its elements has been the subject of countless judgments rendered by experienced courts. The contradictory and critiquing opinions of the learned courts prevented the right to privacy from receiving any specific identification as a fundamental right before 2017. However, following the ruling in the case of ***Justice (Retd) K.S. Puttaswamy***, the right concerning one's secrecy has received widespread recognition, as a vital and intrinsic right and a crucial component safeguarded by Article 21 of the Constitution of our country. The case, also known as the **Aadhar Case**[6], involved a 9-judge bench that rendered a landmark decision granting the need for privacy rights, an individual standing.

The case was initiated in 2015 before a three-judge bench, and the issue at hand was the legality of the Aadhar database and the information that was obtained from an individual's Aadhar by other entities and organizations. The state questioned the inherent privacy rights and its eligibility for a distinct and independent status as a fundamental right. In this case, Justice K.S. Puttaswamy, a retired judge of the Karnataka High Court, filed a writ petition upholding a challenge to the legality of the government's compulsory Aadhar system. He said that the growing usage of Aadhar is violating everyone's privacy because it intends to divulge a person's original information to numerous government and business sector entities.

The court issued many orders in this matter. The bench ultimately decided that an individual's right to privacy is one of the constitutional and indispensable rights guaranteed by Article 21 mentioned in the Constitution of India and is a part of the

[2] Westin and Alan, **Privacy and Freedom (1967**)

[3] Louis D Brandeis and Samuel D Warren II, ***Right to Privacy (1890)***

[4] (Central Information Commission - *Report on Right to Privacy*)

[5] ***Special Rapporteur on Right to Privacy***, Cannataci, J.A. 2021

[6] Justice K.S. Puttaswamy (Retd) vs. Union of India and Ors., AIR 2017 SC 4161

Indian Constitution as a whole. The bench continued by stating that Article 21 provides complete guardianship and security for the right to privacy and is an essential component of the rights to life and personal freedom. On behalf of the other judges, **Judge D.Y. Chandrachud** emphasized that maintaining one's privacy is essential to maintaining one's intimacy, relationship, family life, potential to procreate, social life, and sexual life. He also stated that although privacy may be used for both public and private purposes, we must always safeguard it at its core and ensure that it is never given up to anyone else. This is because privacy is a component of an individual's dignity, and if it is taken away, the person loses all of his or her dignity.

The ***Maneka Gandhi vs Union of India***[7]**,** the case is yet another significant ruling about the right to privacy. Maneka Gandhi, a social activist, and politician filed a petition in 1978 alleging that her privacy and personal freedoms had been violated when the Indian government impounded her passport and denied her a fair opportunity of being heard. She also petitioned the Apex Court to stop the unfair conduct of the government, claiming that they had infringed both her freedom to travel and her right to personal liberty. As per the rulings of the Supreme Court, the right to privacy under Article 21 emanates from personal freedom and liberty of thought. In addition, the bench held that it is not a truly free right and may be subject to constraints based on the legal procedure as well as government acts taken to protect national security, public order, and morality. The court also decided that any restrictions on the freedom of privacy must be reasonable and not arbitrary.

The ruling, in this instance, was issued by a seven-judge bench, and it upheld the essence of justice by recognizing the validity of the right to privacy and introducing the golden triangle rule. The court said that any regulation that limits someone's freedom and liberty must withstand the reasonableness test under Articles 14, 19, and 21 of the Indian Constitution.

Privacy and Sexual Orientation

Similarly, the ***Naaz Foundation case***[8] also threw light on the aspect of protecting one's privacy. The High Court of Delhi ruled in 2009 and issued a historic decision that decriminalized homosexuality in India. Although the case mainly highlighted conflicts with the IPC's Section 377, which criminalized consenting same-sex relationships, it also raised issues with privacy rights. The court ruled that sexual orientation is a crucial component of the right to privacy, which is a fundamental liberty protected by the Indian Constitution. The court additionally determined that section 377 was unconstitutional considering that it violated the rights of homosexuals to their privacy and dignity. The court held that any form of discrimination based on gender identification would go against the right to equality. In this instance, it was acknowledged that the right to privacy encompasses the freedom to decide to act about one's body, sexuality, and interpersonal relationships in addition to the right to be left alone. As it prepared the path for more acceptance and acknowledgement of their rights, it was also a landmark triumph for the LGBTQ+ community in India.

In a different incident in 2018, with the recognition that the right to sexual preference and gender identification are fundamental rights protected by the Indian Constitution, this decision made by Justice Chandrachud decriminalized adult consensual homosexuality and legalized homosexual behaviour between consenting adults. Justice Chandrachud made a similar observation about how sexual privacy is a fundamental component of individual freedom. He stated "Whatever a person does to his or her privacy entirely falls under the purview of personal autonomy"[9] and that there shouldn't be any limitations on the privileges of any individual when it comes to his or her sexual choices.

Privacy and Telephonic Communications

Another notable highlight was the ***People's Union for Civil Liberties (PUCL) case***[10], in which the issue of a person's private telephone rights was questioned. PUCL, a non-governmental organization dedicated to advancing civil rights, and other activists initiated the suit in 1996 to contest the government's practice of monitoring phone conversations and communications. The Supreme Court of India first considered the matter in a three-judge panel, which maintained the government's right to intercept communications under the Telegraph Act of 1885. However, a larger bench with nine judges was eventually assigned to hear the case.

The Supreme Court ruled that telephone conversations are a component of a person's freedom of privacy and cannot be intercepted by the government without a legitimate reason. The Indian Constitution's Article 21 protects fundamental rights,

[7] Maneka Gandhi vs. Union of India & Anr. AIR 1978 SC 597
[8] Naz Foundation vs Govt. of NCT of Delhi 160 Delhi Law Times 277 (2009)
[9] Navtej Singh Johar vs. Union of India, AIR 2018 SC 4321
[10] People's Union for Civil Liberties vs UOI and Anr. SC 568 AIR 1997

including the right to privacy, according to a nine-judge Supreme Court bench's declaration in 2017. The court determined that everyone has the right to privacy, which the state is required to uphold with all appropriate safeguards. The decision in the PUCL vs. UOI case has enormous ramifications for India's privacy rights which has been praised as a major win for civil liberties.

Right to Privacy and Speech and Expression

The following remark may be drawn from another case known as the ***"Auto Shankar Case."***[11] The case started in 1988 when R Rajagopal, a Tamil-language magazine editor, wrote an article saying that a wealthy businessman called S Varadarajan has connections to an infamous criminal known as Auto Shankar. In 1990, the Madras High Court directed the magazine to pay Varadarajan damages after Varadarajan filed a defamation lawsuit against Rajagopal. Rajagopal, however, filed an appeal with the Supreme Court after being dissatisfied with the Madras HC's decisions. In 1994, the SC handed down a significant ruling in his favour that outlined the parameters of free speech and expression in India. The court decided that the right to privacy was a pressing component of human freedom and could not be violated unless it was necessary for the sake of public morality, decency or national security. The court further decided that the journalist's voicing himself and expressing one expression did not outweigh the businessman's right to privacy, and as an outcome, the article could not be published without the businessman's permission.

Potential Threats to Privacy on Social Networking

Social media has completely transformed the demeanour in which we engage and exchange words with one another, but it has also raised privacy issues. When we use social media platforms, we frequently share personal information with a large audience, and if the information is mishandled, it might have major repercussions. Users of social media have expressed worries about privacy in recent years. A troubling scenario has arisen among many users in past years as a result of data breach instances, which led users to reconsider their social media relationships concerning their privacy.[12] However, despite the policies which these social media platforms provide, claiming to protect our privacy, there are several examples where the reports show that these organizations fall short in protecting our data. Data Breaches, Tracking and Profiling, Social Engineering, and Phishing Attempts are some of them.

Listed below are some ways that social media may affect our privacy:

1. **Information Gathering:** Social media networks gather a huge amount of information about their users, such as their locations, browsing history, and individual preferences. This data can be sold to other parties or used in other ways, in addition to being used to target advertising.
2. **Public Sharing:** Several social networking platforms make our information public by default, making it available to everyone. Personal data like name, address, past whereabouts, chat logs, and contact details are included in this. This makes our personal information available to everyone, thus violating our privacy.
3. **Cyber Bullying:** Social media may be a fertile ground for cyberbullying since users can lurk behind anonymous profiles and utilize these platforms to harass or threaten others. This fosters misidentification about those who harass others by using many accounts while concealing their identities.
4. **Security Threats:** Social media networks are susceptible to hacking and other security flaws that might reveal your personal information to strangers. This might result in data being used by unauthorized users, who might misuse our private information and use it to blackmail others to unfairly extract money from them.
5. **Tracking and Monitoring:** Social networking sites frequently employ monitoring software to keep track of our online activity and create profiles of us. Following that, this profile can be used to sell to other businesses or to target us with customized adverts. By monitoring our geolocation, camera, and audio records, these organizations maintain tabs on our behaviour.
6. **Surveillance and censorship:** Social media platforms may be used by governments and other groups to monitor our online actions and restrict the information we have access to, which makes them a potential tool for surveillance and censorship. This surveillance can take many forms, including the use of automated tools to scan social media posts, the use of human analysis to monitor specific individuals or groups, and the collection of data about our social activity.
7. **Phishing:** The most typical method of obtaining someone's sensitive information is phishing. It is a kind of cyberattack that entails delivering false communications to target individuals to fool them into giving over

[11] R Rajagopal vs State of Tamil Nadu 1994 SCC (6) 632

[12] Tulane University School of Professional Advancement, "***Social Media Privacy Issues for 2020"***

sensitive data, including login passwords, banking details, and other personal information. In such assaults, harmful URLs, impersonation, fictitious login pages, and account takeover are used.

8. **Malware Sharing:** Malware sharing is the dissemination or exchange of harmful software, frequently to corrupt or endanger the security of the devices of other users. After a malware program has been added to a recipient's program, it may be used as a tool to extort money from users by serving up offensive adverts or to collect sensitive information. Social media platforms are leading the way in disseminating these malicious programs. It may be done through a variety of techniques, including email, attachments, and file-sharing websites.
9. **Botnet Attacks:** Botnet attacks are specific kinds of cyber-attacks in which a botnet, or network of hacked computers, is used to launch a planned attack against a target. Social media bots are automated accounts set up for harmful purposes that generate new profiles, follow new users automatically, and publish content. Malware includes spam, data theft, and distributed denial-of-service (DDoS) operations, all of which are methods used by cybercriminals to access user accounts and communication networks.

To protect against these harmful operations, users should be cautious about clicking on suspicious links or downloading unknown files. The sharing of sensitive data and financial credentials must be avoided by the users to safeguard their privacy.

Instances of Social Media Privacy Infringement

On social networking platforms, there have been many well-publicized privacy breaches. A social media privacy breach may have long-lasting implications, such as identity theft, fraud, and reputational harm. The exposure of personal information is the first significant effect of a privacy violation on social media. The harm to one's reputation is another significant effect. Social media platforms are open forums where anybody may view any material posted there. An individual's reputation may suffer if intimate or humiliating information is made public. When the issue involves businesses or other entities, it may directly affect customer trust and loyalty, which may finally result in a loss of business.

The **Cambridge Analytica Controversy**[13] started with the personality test "This is your digital life," which was developed by Aleksandr Kogan, a Cambridge University researcher, and which made headlines in March 2018 when it was revealed that the corporation had gained millions of Facebook users' personal information without their knowledge. Cambridge Analytica worked on the Donald Trump campaign during the 2016 US presidential election. The software was developed with the intention of gathering information on Facebook users, including their likes and interests as well as those of their friends. Thereafter, Kogan sold this information to Cambridge Analytica, which subsequently utilized it to produce precise political advertisements for the Trump campaign. Following the revelation of the event, Facebook CEO Mark Zuckerberg was called to appear before Congress where he was confronted with difficult questioning regarding the firm's data policies and its involvement in the election. After the controversy, Facebook made a number of adjustments to its data practices and policies. Many individuals were made aware of the value of securing their personal information online amid the Cambridge Analytica controversy. Furthermore, it emphasized the necessity of social media companies exhibiting greater responsibility and openness.

In 2020 a privacy scam named **"Twitter Privacy Scam"**[14] targeted Twitter users with hackers using a fake verification process to gain access to users' accounts and personal information. In order to pull off the fraud, users were sent direct messages that claimed to be from the Twitter support team requesting them to click on a link and enter their account credentials to authenticate the account. Hackers were able to access users' accounts and personal information once they clicked on the link and inputted their information. The target audience for the fraud was individuals who were already worried about their privacy, security, and usage of social media, which was particularly alarming. Using branding and logos that mirrored those on Twitter's website, the false verification procedure was made to appear genuine. In response to the privacy fraud, Twitter urged users to exercise caution and flag any unusual behavior on their accounts. In order to safeguard consumers' privacy, the company also introduced extra safety preventative measures, including two-factor authentication and login verification.

---

1. [13] Nicholas Confessore, ***Cambridge Analytica and Facebook: The Scandal and the Fallout So Far,*** N.Y. Times, April 4, 2018.

[14] Joanne Berman, Jonathan Blattmachr, Debra Brookes, Shirin Emami, Robert Francis, Marcia Henry, Justin Herring, Matthew Homer, Katherine Lemire, Sasha Mathew, Chris Mulvihill, and Richard Weber, ***Twitter Investigation Report, Department of Financial Services,*** New York (.gov), 14 October 2020.

In 2018, a reported scam took place on the part of Google where Google announced a privacy Breach that had exposed the personal data of thousands of Google+ users. The breach unfolded between 2015 and 2018 and was brought on by a software vulnerability that gave access to user profiles to outside developers even when the privacy setting for those profiles was private. Users' names, email addresses, professions, gender, ages, and locations were among the data that were exposed, although more critical information like passwords or financial information was not among them. Several lawmakers and privacy advocates criticized Google for how it handled the privacy breach and demanded openness and accountability from the corporation. In retaliation, Google reached a settlement with the Federal Trade Commission for the privacy breach for $170 million, the highest payment ever paid by a tech corporation. The agreement obliged Google to establish more stringent privacy safeguards and to submit to annual privacy audits for the following 20 years.[15]

Protecting Privacy in the Digital Age

Privacy on social media is a growing concern for many people, as more and more personal information is being shared online. However, there are several methods you can use to safeguard your privacy on social media. Here are a few ideas:

1. **Review your privacy settings:** You can usually manage what information is posted and who may access it on social networking sites. Check your privacy settings and adjust them as needed.
2. **Constrain the quantity of private information you divulge:** Think carefully before sharing any private information on social media. Avoid sharing sensitive information such as your full address, phone number, or financial information.
3. **Be careful whom you add as friends on social media:** Be selective when adding people as friends. Accept friend invitations only from persons you are mutually connected with or who you really know in person.
4. **Use strong passwords and activate two-factor authentication:** To add an additional layer of protection, use strong passwords that are unique for each social media account.
5. **Employ a pseudonym:** Instead of using your own name on social media, think about adopting an alias or a pseudonym. This may enable you to preserve some of your privacy and anonymity.
6. **Consider your options carefully before posting:** Before sharing any material on social media, consider if you want it to be seen by the public. If in doubt, it is best to stay safe and refrain from posting.
7. **Steer clear of dubious links:** Refrain from clicking on links from unreliable sources. These links can lead to malware that compromises your security and privacy, or they might be phishing schemes.

We can protect our privacy on social media and have a safer online experience by adhering to these guidelines. It is therefore required for everyone to be cautious while using these social networking sites as they are prone to be harmful to our privacy and it is our duty to protect it.

Conclusion

The protection of privacy is a complex and evolving issue. Individual rights, community interests, and technical improvements must all be carefully taken into account when addressing the complicated and always-changing subject of privacy protection.

Privacy is a fundamental right that should be protected. Individuals are entitled to regulate how their personal information is used, shared, and accessed. Several legal and regulatory structures, such as privacy and data protection laws, are in place to safeguard privacy. These frameworks must, however, be upgraded and improved on a regular basis to keep up with advancing technology and shifting social mores. In order to maintain privacy, knowledge, and education are essential. Individuals must be mindful of potential hazards and take precautions to protect their personal data, including using secure passwords, refraining from revealing private information online, and being cautious when installing apps and software.

In essence, maintaining privacy is a complex subject that calls for constant attention and effort from individuals, groups, and governments. While there are no quick fixes, we can guarantee that privacy is still a basic right in the digital era by joining together and remaining vigilan

REFERENCES

BOOKS

- Westin and Alan, **Privacy and Freedom (1967**)
- Louis D Brandeis and Samuel D Warren II, ***Right to Privacy (1890)***

2.

3. [15] Douglas MacMillan & Robert McMillan, ***Google Exposed User Data, Feared Repercussions of Disclosing to Public,*** The Wall Street Journal, October 8, 2018.

REPORTS

- (Central Information Commission - *Report on Right to Privacy*)
- ***Special Rapporteur on Right to Privacy***, Cannataci, J.A. 2021

CASES

- Justice K.S. Puttaswamy (Retd) vs. Union of India and Ors., AIR 2017 SC 4161
- Maneka Gandhi vs. Union of India & Anr. AIR 1978 SC 597
- Naz Foundation vs Govt. of NCT of Delhi 160 Delhi Law Times 277 (2009)
- Navtej Singh Johar vs. Union of India, AIR 2018 SC 4321
- People's Union for Civil Liberties vs UOI and Anr. SC 568 AIR 1997
- R Rajagopal vs State of Tamil Nadu 1994 SCC (6) 632

ARTICLES

- Tulane University School of Professional Advancement, "***Social Media Privacy Issues for 2020"***
- Nicholas Confessore, ***Cambridge Analytica and Facebook: The Scandal and the Fallout So Far***, N.Y. Times, April 4, 2018.
- Joanne Berman, Jonathan Blattmachr, Debra Brookes, Shirin Emami, Robert Francis, Marcia Henry, Justin Herring, Matthew Homer, Katherine Lemire, Sasha Mathew, Chris Mulvihill, and Richard Weber, ***Twitter Investigation Report, Department of Financial Services,*** New York (.gov), 14 October 2020
- Douglas MacMillan & Robert McMillan, ***Google Exposed User Data, Feared Repercussions of Disclosing to Public,*** The Wall Street Journal, October 8, 2018.