International Journal of Scientific Research in Modern Science and Technology
ISSN: 2583 -7605 (Online)
© IJSRMST | Vol. 4 | Issue 10 | October 2025
Available online at: https://ijsrmst.com/
DOI: https://doi.org/10.59828/ijsrmst.v4i10.385

Data Privacy while using Social Media Platforms

Dr. Sonali Sagar Gholve

Assistant Professor, Department of Computer Science, Sarhad College of Arts, Commerce and Science, Katraj, Pune. Savitribai Phule Pune University, Pune, Maharashtra, India.

Email: sonalisagargholve@gmail.com

ABSTRACT

Social Media platform is one of the needs of everyone in today's 2025 digital world. Different social media platforms are available and the number of users are very large on all sites. This indicates that privacy issues are also more when users increase and sensitive information is transferred. This study explains about the Digital ecosystem and types of data, data collection, Data ripple effect and data brokers mainly. Social Media platforms work starts with Data collection and ends with ripple effect and Privacy. Security threats need to be identified and to create awareness about privacy. Study focuses on privacy toolkit, different platforms privacy settings. Recommendation to users, regulators and social media platforms.

Keywords: *Social Networking Sites (SNS), Data Privacy, Privacy toolkit, Data Collection, Advertising, Digital footprints.*

Introduction

When the internet entered human life around 1983, worldwide communication was possible quickly. Email is the first seed of a social media platform. Social media is the platform to exchange user generated contents. Social media platforms used for different purposes like celebration, promotions, clubs, information sharing etc.

Social Media Platforms

According to the data available on GWI 96.9 percent people (age above 16 and below 54) using social media platforms either for posting or for communication. Data varies because duplicate accounts exist and age restriction of some platforms. Average use of social media platforms is 15 billion hours every day. We can’t predict the single name of mostly used social media because everyone's perspective is different to use that platform. According to GWI research facebook (56.9% user) is the most popular social platform. 55.4% users are using Youtube for videos. For the communication purpose whatsapp is in 3rd rank with 38.45 users using it as messenger.

IJSRMST | Received: 13 October 2025 | Accepted: 29 October 2025 | Published: 31 October 2025

Digital Ecosystem

The concept of data privacy concerned with every digital interaction. Digital interaction is the base of data privacy. Digital footprint means obvious and subtle data of the user's record while using the internet. In digital footprints there are 2 types of traces Active Data and Passive data.

Active Data

It includes direct involvement in action like publishing posts on media, comments on thread, submitting information online etc.

Passive data

This is more dangerous, because the user is unaware about the submission of data. This data collection through cookies, browsing history, location data through background activities, device details etc. So we can say digital footprints means crucial details collected by third party data brokers through online activity. It's important for an organisation to take care of the digital footprint of employees. Digital footprints can be increased due to Cloud migration and remote work. Cyber criminals are targeting the employees through different footprints like email, company websites, device applications etc.

The Data Exchange

All social media platforms are free to use. They are providing free services but the main aim is different, they are collecting the data of users. In reality the user is the main product here, users buy with data and data sold with money.

Advertising

Social media platforms collecting demographic and behavioural information from users and generating revenue through advertising. They are sharing this information with advertising partners. Then the partner will analyse the data and similar product advertisements will be visible to that user on his account.

Objectives

1. To know the usage of Social Media platforms.
2. To Understand Data Privacy.
3. To understand data collection and usage via social media platforms.
4. To know the ripple effect of data collection.
5. To learn the privacy settings.
6. To find corrective actions for social media use.

Literature Review

According to the author Kumar (2016) people enjoy the information sharing on the internet but it's opening the back doors to privacy and security. People present their own private information and create difficulties for themselves. The main risk of sharing data is information disclosure[1].

Monetization practices: Social media platforms are selling the Collected data to different resources. Social networking sites have many benefits but also have some negative angles like excessive use of sites, changes in behaviour, and negative effects on wellbeing(Wang et, al 2022)[3].

According to the Surfshark (2023) report Facebook, YouTube and Instagram were banned in countries like China, Iran and Turkmenistan for 14 years(APU).

According to APU there are positive effects of social media: Having a platform to express yourself, improvement in mental health, professional networking increased, Social awareness, educational opportunities, promoting business etc.

Jiyauddin (2024) founded the Legal framework for privacy protection: InformationTechnology Act 2000 providing rules and regulation to provide safeguard to personal data. To protect the data, the government established the Data Protection Authority of India (DPAI).

According to the ministry of law and Justice in India the Digital personal Data Protection(DPDP) act, 2023 exists to process personal data. A Personal data Protection Bill is also there but it is waiting for parliamentary approval.

Research Methodology:

Different web sources and papers examine to collect data.

Data Collection

Social media not only collects biographical details but also collects data through tracking cookies, geofencing, browser fingerprinting, deep insight into personal life, close friends, location and interest.

Social media collects data via device permissions and tracking techniques. Explicit Data collection through the posts, comments and likes. Instagram using AI and big data and finding the posts or shares by users previously, based on this instagram will tailor the data for that user.

Data collection table by social media

Category	Information collected	Purpose
Persons Basic info	Name, age, Gender, birth date, address, Contact number	Authentication and profile building
Device and connection	Ip address, network type, speed, device type	Security, fraud detection and targeting ads
Internal data- Behavioral	Post, shares, likes, comments, time spent	Training AI, Understanding interested area
Hidden/ Off site data	Tracked via cookies	To build detail profile
Sensitive data	Address book, messages, drive access, history	Detailed profiling and targeting

Ripple effect of data collection

Data collection is not an issue but it is the first step. The issue is generated when Collected data is processed and sold, it will affect personal security, financial assessment.

Data Brokers

The specialize entities which buy consumer data elements. These are collecting the data through various social media platforms, websites, public records, apps etc.

Dossiers

Detailed personal profile build based on collected data for the marketing purpose. Data posted on social media will be data points for the different government agencies, advertisement companies, insurance companies, political campaigns, to check new voters.

The Risks of Algorithmic Profiling

1. **Financial Scoring:** Different insurance and loan companies using the collected data of different platforms while giving the loan. The persons in the age group of 25-34 found that social media platforms affected negatively on their premium and loan.
2. **Black Box Problem**: Consumer having no idea of non- financial points, there is no transparency and correct potential to challenge.

Security threats

1. **Overshairing**: It will cause the personal information to miss use and also physical risks when the data is shared about the current locations like holiday plans or picnics. Thieves will get clues of home emptiness.
2. **Reputation:** Old posts or data may be used to damage your current reputations. The data will exist for a long time so just by finding a person's old data someone can use it to damage one’s reputation.
3. **Echo chamber effect**: The individual will feel that all opinions are like his opinion only.

Privacy Toolkit

1. **Unique Password:** Keep different passwords to different accounts. Passwords must be easy to keep in mind but difficult to crack.
2. **2FA:** Two factor Authentication Separate verification code will be sent on mobile or email. It will work as a security barrier for hackers.
3. **Device and account strategy**: It is important to lock devices with fingerprints or face detection. When a device is in the wrong hands it will cause a big entry to hackers. Logout social media app when they are unused on your device. Delete unused accounts because these are safe doors for attackers to hack your accounts.

Privacy settings

Social media platforms provide privacy settings while sharing the data, but most of the time by default privacy settings are public, users need to change it. We can not categorize privacy, but need to understand to what extent we can reveal the data.

1. **Visibility Settings**: platform providing the setting to users while posting content. Users can lock profiles for general search. Users can hide posts from specific groups of people and restrict the data visibility.
2. **Location settings**: Users need to offer location sharing; it will create physical risks of sharing live locations. Users need to stop device level location tracking.
3. **Advertising Personalization**: Users need to check the setting to allow your content for advertisement or not. Users need to disable these features of using profile data for advertisement.

Privacy settings need to be done in Social Media platforms

According to recent study 100's of social media platforms are there but some are most popular and here setting options of them discussed here.

Facebook: Here users can hide the profile in general search using different visibility like Public, private, only friends etc.

Facebook: Click on profile icon on right side of window -> click on settings and privacy -> Privacy checkup

Different options available are-

- Who can see what you share?
- How people can find you on facebook.
- your data settings on facebook.
- Keep your account secure-Facebook providing different recommendations under this

  This will provide options for account password and security. Options available for login, password management and recovery methods.

YouTube: Click on the left side collapse menu to see the option of settings-wheel icon->Permissions-> manage permissions.

If user wants to change visibility of videos : click on profile Icon -> your videos-> select video-> change visibility (Public, Private, Unlisted)

Instagram: on the left-hand side of the window-> click on More-> Settings-> Account Privacy-> Change visibility to Private account on/off. When the account is private only followers can see the post and details but when the account is public anyone can see the posted material.

WhatsApp: Click on the wheel icon/ Settings->Privacy

Here users can manage the options like who can see your profile, and other details like last seen, IP address, App lock etc. Also check for Privacy checkup

Smart Sharing - Privacy Management

1. **Knowledge of Sharing**: It's important to understand which data to be shared. Avoid sharing the current location, detailed home address, contact information etc.
2. **Data separation**: It is necessary to maintain separate accounts for personal and professional data. So accurate information will reach the right audience.

3. **Data Boundaries:** Setting the boundaries is the important tool to secure your data from spam, and unwanted followers.

Results/Findings

There are some negative aspects of social media like cyberbullying, Addiction, Doxxing etc.

Privacy protection using technology: With the help of encryption techniques we can protect the data. By controlling access to data, only authorized persons can access sensitive data. Anonymization of data so no one's identity will leak. With the help of data minimization we can protect the data, collect only required data to avoid data breach. Use safe data storage procedures like firewall or intrusion detection systems. Regular security audits are required to find weaknesses(Jiyauddin(2024)).

Conclusion and Recommendations

To users: Need to take corrective actions for use of social media like switching to different technologies, reduce the usage and break in using the sites[3]. This study focuses on how to reduce use of social networking platforms and how to preserve privacy and avoid future problems like addiction and behavioural changes due to excess use of SNS.

Reduction in use is a solution to privacy . Then who can help to rescue use of Social Media Sites(SNS)? Parents and family members can control wards for reducing the use of SNS. Organizations can help or put restrictions on using the SNS during work time. SNS also helps users to reduce the use for the reason of ethical and legal issues.

For Social media Platforms: Need to raise awareness about data Privacy. Strict age rules and authentication for usage of social media. Need to recommend the privacy settings. Reminders for frequent password change. Compulsory actions required to learn Terms and Conditions.

Obtain user Consent: Before using any users data platform needs user consent for the same.

Need to provide data breach notice. Users have the right to use the old or new data and to share or download it. He can post data according to his wish, there will not be any probability / restrictions Chandra(2023).

For regulators: The Ministry of electronics and information Technology (MEITY) needs to formulate strict policies and actions regarding the digital platform and internet.

The press information bureau needs fast fact checking units to verify the misinformation spreading over the internet. Also need to keep watch on telecommunication services which are also included in data privacy. It will create a big impact on social media platforms.

References

[1]. Kumar, Senthil & Kandasamy, Saravanakumar & K, Deepa. (2016). On Privacy and Security in Social Media – A Comprehensive Study. Procedia Computer Science. 78. 114-119. 10.1016/j.procs.2016.02.019.

[2]. Rewaria, Sakshi, Data Privacy in Social Media Platform: Issues and Challenges (February 26, 2021). Available at SSRN: https://ssrn.com/abstract=3793386 or http://dx.doi.org/10.2139/ssrn.3793386

[3]. Wang, H., Miao, P., Jia, H., & Lai, K. (2023). The Dark Side of Upward Social Comparison for Social Media Users: An Investigation of Fear of Missing Out and Digital Hoarding Behavior. Social Media + Society, 9(1). https://doi.org/10.1177/20563051221150420 (Original work published 2023)

[4]. Dari, Sukhvinder & Dhabliya, Dharmesh & Govindaraju, Kaladi & Dhablia, Anishkumar & Mahalle, Parikshit. (2024). Data Privacy in the Digital Era: Machine Learning Solutions for Confidentiality. E3S Web of Conferences. 491. 10.1051/e3sconf/202449102024.

[5]. Mr. Md Jiyauddin(2024), Technical and Legal Aspects of Data Privacy in India: A Critical Analysis With Legal Provisions**,**Volume 2, Issue 4, IJLSSS, **PP** 01 – 10

[6]. A. A. N. Al-Rabeeah and F. Saeed, "Data privacy model for social media platforms," *2017 6th ICT International Student Project Conference (ICT-ISPC)*, Johor, Malaysia, 2017, pp. 1-5, doi: 10.1109/ICT-ISPC.2017.8075361.

[7]. Chandra (2023) The Ethics of Social Media Privacy: User Rights and Responsibilities, INTERNATIONAL JOURNAL OF RESEARCH CULTURE SOCIETY, Monthly Peer-Reviewed, Refereed, Indexed Journal , Volume - 7, Issue - 9, September- 2023, DOIs:10.2017/IJRCS/202309001 .

[8]. https://www.apu.apus.edu/area-of-study/business-and-management/resources/how-social-media-sites-affect-society/

[9]. https://www.gwi.com/?utm_campaign=FY25_CC_ALL_GL_KEPIOS&utm_source=partner&utm_medium=kepios&utm_term=report_content

[10]. https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

[11]. https://epic.org/issues/consumer-privacy/data-brokers/

[12]. https://www.terry.uga.edu/how-social-media-posts-could-affect-credit-scores/

[13]. https://www.firstbank.com/resources/learning-center/the-risks-of-oversharing-what-you-need-to-know-about-social-media-privacy/

Cite this Article:

Dr. Sonali Sagar Gholve, “Data Privacy while using Social Media Platforms”, *International Journal of Scientific Research in Modern Science and Technology (IJSRMST), ISSN: 2583-7605 (Online), Volume 4, Issue 10, pp. 27-33, October 2025.*

Journal URL: *https://ijsrmst.com/*

DOI: *https://doi.org/10.59828/ijsrmst.v4i10.385*.