Volume 11, Issue 4, April – 2026 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr1260

Study of Privacy Features in Social Media Applications

Awareness of Privacy Features

Akanksha Shyamdhar Mishra[1]

[1]Assistant Professor, Department of Information Technology Shankar Narayan College of Arts & Commerce, Bhayander, Maharashtra, India

Publication Date: 2026/04/22

Abstract: Social Media, an online platform where user can create, share and interact with the content and the people. Social media applications, such as Facebook, Instagram, Twitter, and Snapchat have become all-over in our society and are essential parts of our daily communication. These apps allow users to post and share personal information, media, and thoughts with anyone in the world. However, the increasing popularity of social media sites has caused concern over the safety and privacy of user data. In this study, I have investigated the privacy protections of major social media sites and discussed their effectiveness in ensuring user privacy. I have surveyed 50+ people about awareness of Privacy Features in Social Media Applications. This research reveals that while a variety of privacy mechanisms exist to protect user data, many users are either unaware of them or unwilling to use the available options. Security breaches and data exposure remain significant risks in the use of social media sites. This study will discuss the gaps between the current design of privacy settings in social media sites and the actual privacy practices of those users.

Keywords: *Social Media, Privacy, Applications, Features, Awareness.*

How to Cite: Akanksha Shyamdhar Mishra (2026) Study of Privacy Features in Social Media Applications. *International Journal of Innovative Science and Research Technology*, 11(4), 1555-1560.
https://doi.org/10.38124/ijisrt/26apr1260

I. INTRODUCTION

Social media applications are becoming a basic part of the digital era, altering how people interact, share information, and communicate with each other. Social media platforms such as Facebook, Instagram, Twitter, and Snapchat connect users worldwide, allowing them to share ideas and create online communities. These platforms not only connect users but give users the opportunity to share personal information, photos, videos, opinions, and real-time updates about themselves with friends and followers and with non-followers too. They are making communication quicker and more efficient. However, the sharing of personal information has led to significant concerns about privacy and data security.

Social media privacy is the capacity of users to control the manner in which their personal data is accessed, utilized, and shared by these platforms. With the ever-increasing amount of data that is being created daily, social media companies have incorporated several privacy features to ensure better data security and protect users' confidential information. These privacy features facilitate users to manage their personal data actively.

Some of the key privacy features available in social media applications are profile visibility settings, which allow users to choose who can view their profiles and posts; audience selection tools, which enable users to control the visibility of individual posts; and friend or follower management options, which help users manage their connections. Additionally, advanced security measures such as data encryption protect sensitive information from unauthorized access, while two-factor authentication adds an extra layer of security to user accounts. Permission settings also allow users to control access granted to third-party applications like camera, locations and also websites.

Even though there are many privacy features available many users are not aware of it. Due to by default settings many data are exposed and accessed publically to public who do not even know the unaware users. Some apps have complex privacy policies and confusing user interface makes user difficult to understand its privacy features how their data are being used.

Another main things here in social media platforms are data transparency and accountability. Social networking sites must be held accountable for security and privacy, but this is on them to the extent that they implement robust security and

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr1260

clearly articulate their data usage policies. In the past, some sites have apparently abused user data and/or do not adequately secure privacy settings, resulting in a lack of trust.

II. METHODOLOGY

Social media platforms which are Internet-based services allow users to create, share and interact with content, is a main factor of this study. It focuses on users' awareness and the efficiency of privacy settings in protecting personal information. The research is quantitative and diagnostic in nature. This paper explores user habits and perceptions about privacy settings in the main social media applications.

- *Data Collection*

Primary data were collected using a structured questionnaire distributed to over 50+ respondents. The questionnaire comprised multiple-choice questions designed to evaluate "User awareness of privacy features" shown in Fig. 1.

- *Sampling Technique*

The easy sampling method was used to collect active social media users data on awareness of social media privacy features. The sample included individuals from different age groups and gender to obtain user behaviour data.

- *Data Analysis Techniques*

The collected data are analysed using pie-charts.

- *Ethical Considerations*

All responses from users collected anonymously and confidentiality of data was strictly maintained.

- *Limitations*

Responses are less which results small sample size and limited to less data of awarenesss of privacy features.

III. KEY FINDINGS

The results of the responses gets the major gaps in awareness and usage of privacy features in social media. The findings show that a vast number of users are unaware of the privacy settings available on social media applications such as Facebook, Instagram, WhatsApp, and Snapchat shown in Fig.2 or they do not use these settings even when they are available. This indicates that there is a lack of understanding of the importance and use of privacy control tools offered by social media applications.

If we talk about usage and privacy awareness then WhatsApp stands out. Nowdays Instagram is being most used app but users lack full awareness of advanced features shown in Fig.3.

Even though social media applications offer a range of privacy mechanisms to users, the tools are not effectively used. A large number of respondents stated that they rarely change the default settings of social media applications, which expose their personal data more than intended.

As a result, users' personal data become vulnerable to being accessed and shared without permission. The users are highly at risk of data exposure and security breaches due to lack of awareness and low proactive personal input to privacy settings of social media applications.

IV. MODELING & ANALYSIS

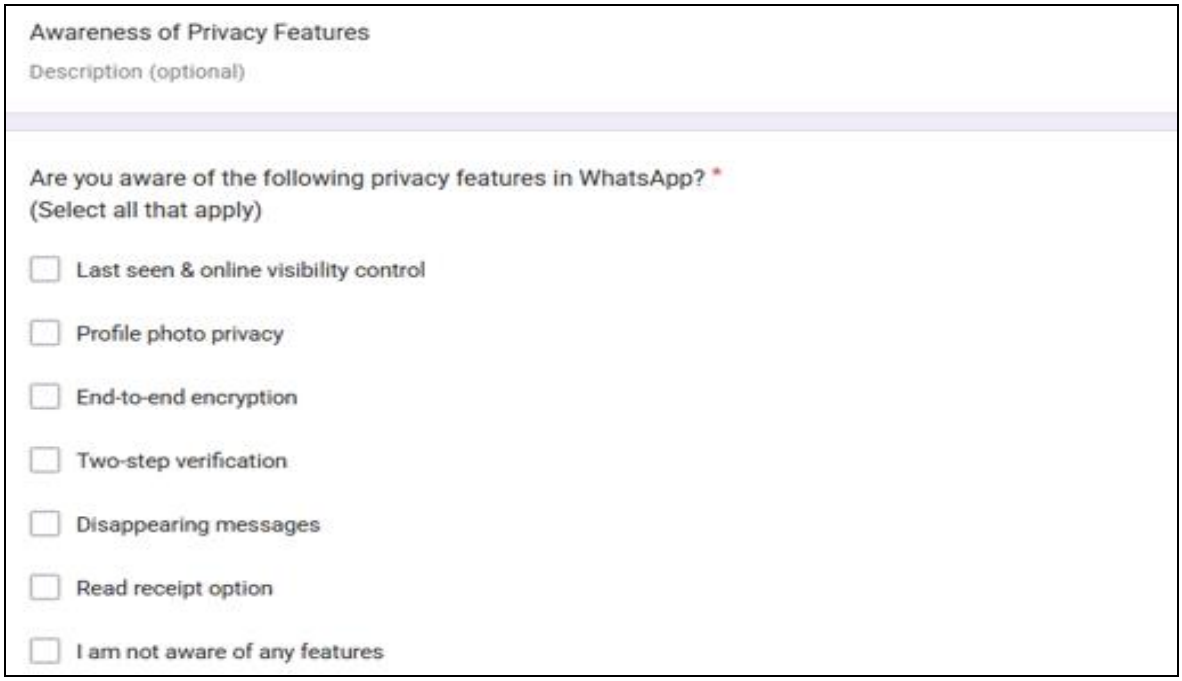

Fig 1 Questionnaire

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr1260

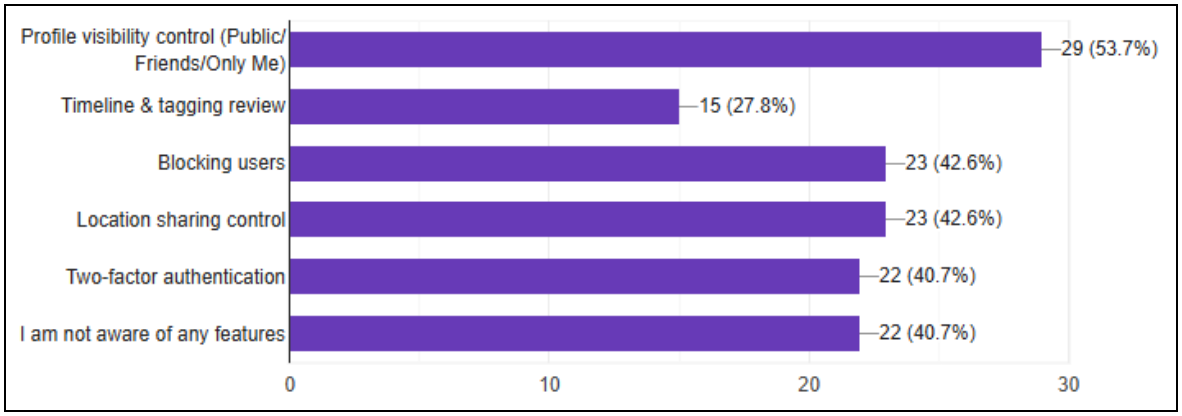

Fig 2 No. of Users Unaware of the Privacy Settings

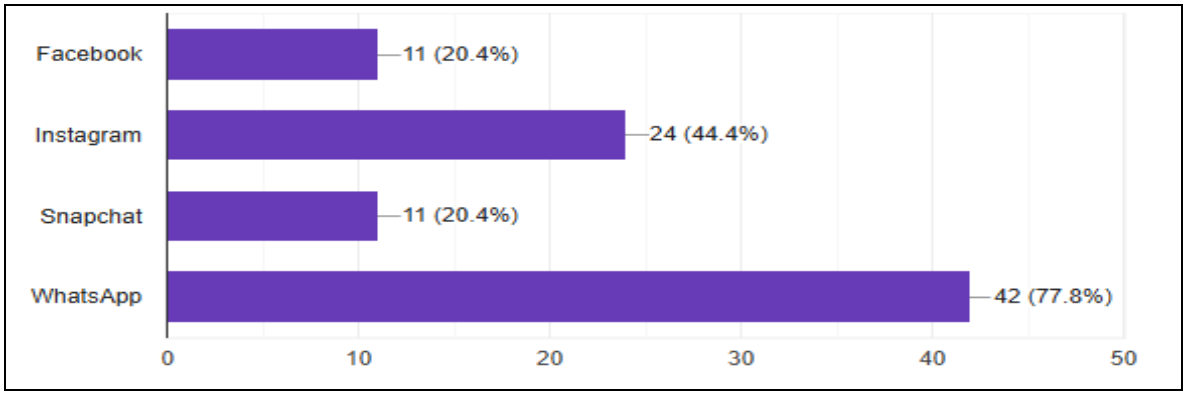

Fig 3 Lack of Awareness

V. DATA PRIVACY ON SOCIAL MEDIA PLATFORMS: WHAT TO KNOW

➢ *Valuable Data*

- Personal Information: Name, email, phone number, and location.
- Behavioral Data: Likes, shares, comments, and interactions.
- Content Creation: Photos, videos, and posts.

➢ *Privacy Settings to Choose who can Access your Data*

- Check Your Settings: Use the "Privacy Checkup" tools to stay on top of your privacy settings.
- Restrict Information Sharing: Restrict sharing personal information such as phone numbers and locations.
- Set Your Audience: Control who can view your posts friends only, specific groups, etc.
- Manage Friend Requests: Only accept friend requests from people you know to prevent fake accounts

➢ *Best Practices to Secure your Data*

- Always enable two-factor authentication (2FA) or multi-factor authentication (MFA)
- Always use complex passwords
- Regularly check recovery email and phone-number. It should be current & secure.
- Never click on suspicious links
- Enable login alerts
- Never share sensitive information like ID, Financial details, Personal Schedule and other sensitive informations.

VI. THINGS TO REVIEW IN PRIVACY CHECKUP

Below are the most used Social media Application:

A. Facebook

➢ *Who can see your Info*

- Control visibility of phone, email, birthday, relationship status
- Manage audience for past & future posts
- Review/block users

➢ *Account Security*

- Update password
- Enable login alerts for unknown devices

➢ *How People Find you*

- Choose who can send friend requests
- Control lookup via phone/email

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr1260

➢ *Data Settings*

- Review/remove apps & websites linked to your account

➢ *Ad Preferences*

- Control what profile info advertisers use
- Manage visibility of your activity (likes, follows) in ads

B. Instagram

➢ *Privacy Setting and Information*

- Make your instagram account private/public
- Turn off/on account suggestion
- Turn off/on activity status
- Manage connected apps or website
- Deleted content adds on Recently Deleted section

➢ *Controlling your Visibility*

- Make account private
- Hide unwanted comments
- Hide unwanted message requests
- Archive posts and highlighted stories
- Restrict / Mute people
- Remove your followers
- Remove mentions/tags
- Limit interaction by editing close friends list
- Turn off Read Receipt
- Temporarily deactivate account

➢ *Reporting*

- Report spam accounts
- Report messages or chats
- Report comments
- Report posts & stories

➢ *Beware of Scams*

- Investment scam
- Romance scam
- Job scam
- Lottery scam
- Collaboration scam
- Loan scam
- Donation scam
- Commerce scam

C. WhatsApp

➢ *Last Seen & Online*

- Choose who can see your last seen and online status

➢ *Profile Photo*

- Set visibility: Everyone / My Contacts / My Contacts Except / Nobody

➢ *About*

- Control who can see your “About” info

➢ *Status*

- Choose who can view your status updates
- Options: My Contacts / My Contacts Except / Only Share With

➢ *Read Receipts*

- Turn blue ticks on/off (except for group chats)

➢ *Groups*

- Control who can add you to groups
- Options: Everyone / My Contacts / My Contacts Except

➢ *Live Location*

- Manage or stop sharing live location

➢ *Blocked Contacts*

- View and add people to block list

➢ *Disappearing Messages*

- Set messages to auto-delete (24 hours, 7 days, 90 days)

➢ *Default Message Timer*

- Set default disappearing time for new chats

➢ *Two-Step Verification*

- Enable PIN for extra security

➢ *Security Notifications*

- Get alerts when a contact’s security code changes

➢ *End-to-End Encryption*

- Messages and calls are encrypted by default

➢ *App Lock*

- Lock WhatsApp with fingerprint/face/PIN

➢ *Linked Devices*

- View and log out of WhatsApp Web/Desktop sessions

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr1260

➢ *Calls Privacy*

- Silence unknown callers

➢ *Advanced Privacy (IP Address in Calls)*

- Protect IP address during calls

➢ *Backup Privacy*

- Manage chat backups (Google Drive/iCloud, encryption option)

➢ *Permissions*

- Control access to camera, microphone, contacts, storage

➢ *Data Sharing*

- Limited sharing with Meta Platforms

D. X (Twitter)

➢ *Who can See your Information*

- Control who sees your posts (public or protected account)
- Manage profile details (bio, location, birthday visibility)
- Block or mute accounts
- Deactivate/Reactivate account

➢ *Account Security*

- Change password
- Enable two-factor authentication (2FA)
- Get alerts for suspicious logins

➢ *How People Find you*

- Control discoverability via email or phone number
- Manage who can send you messages or tag you

➢ *Data Sharing & Activity*

- Review apps connected to your account
- Control data sharing with third parties

➢ *Ad preferences*

- Manage personalized ads based on your activity
- Control use of your data for ad targeting
- Adjust interests and advertiser lists

E. LinkedIn

➢ *Who can See your Info*

- Profile visibility (photo, details, public profile)
- Email & phone visibility
- Connections list visibility
- Activity (posts, likes, comments)

➢ *How People Find & Reach you*

- Who can send connection requests
- Message requests & InMail control
- Profile viewing mode (private/public)
- Search engine visibility

➢ *Interactions & Control*

- Mentions and tags
- Block or mute users

➢ *Data & Apps*

- Download your data
- Manage third-party app access
- Contact syncing settings

➢ *Ads & Preferences*

- Personalized ads control
- Manage interests and advertiser data

➢ *Account Security*

- Change password
- Enable two-step verification
- Login alerts for suspicious activity

VII. HOW NOT TO FALL INTO THE SOCIAL MEDIA PHISHING TRAP

- Never click on links on posts, tweets and DMs unless you're 100% sure that they're legitimate and have good intentions.
- Think before you act when someone approaches you on social media.
- Ask yourself if someone legitimate would even contact you in this way with this information.
- Identify money problems or too good to be true offers for what they really are.
- If you're unsure, call the right number for the person or organisation the tweet or post claims to be from.
- Even if the tweet or post is supposedly from someone you know, their account may have been spoofed or hacked.
- If they've tweeted you, remember that legitimate business accounts usually show a blue 'verified' tick to show their authenticity. They will never ask you for your login details.
- Look at the number of followers the account has. Legitimate organisations ,including their customer support handles will usually have many, many more followers.

VIII. CYBER CRIME PORTAL HELP

https://www.cybercrime.gov.in/ It is an Indian government project aimed at helping victims or complainants file complaints about cybercrime via the Internet. Victims of

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr1260

cybercrime can report any form of cybercrime through this website anonymously. Some of the forms of cybercrimes that one can file reports include hacking, identity theft, online scams, and cyberbullying. This portal helps the public in reporting cyber crimes against women and children. Victims of cybercrimes can use this website to file their complaints, upload evidence, and follow up on their complaints. The National Cyber Crime Reporting Portal also has several tools to help citizens in preventing cybercrimes from happening. The National Cyber Crime Reporting Portal will help protect the cyber environment and create awareness regarding cybersecurity. Law enforcement agencies manage this portal. Any complaints received on this website are investigated and prosecuted by law enforcement agencies/policemen according to the facts in the complaints. Victims must give accurate and detailed information when filing complaints to enable prompt action against the offender.

IX. CONCLUSION

Social media platforms have several privacy settings, which are available and designed to help users protect their personal data and privacy. Nevertheless, the findings from a survey of over 50 participants suggest that there is a substantial gap between the availability of social media privacy settings and user awareness and use of these settings. This neglects user privacy and exposes users to several privacy risks such as data exposure, data misuse, and unauthorized data access. The survey demonstrates that many participants were either unaware or did not fully understand these privacy settings, which directly impacts their use. The findings also suggest that participants often choose convenience over privacy, and prefer to follow default privacy settings without enabling or understanding privacy settings. The findings of this study reveal that there is a huge gap between the availability of these privacy settings and the user's awareness and use, which leaves users exposed to privacy risks. These findings are important because they reveal a disconnect between the design of these privacy settings by social platforms and actual user behaviour. However, social media platforms have made significant efforts to improve the privacy settings available for users. It is important that these platforms continue to invest in user education and simplify privacy settings so that users fully understand them

ACKNOWLEDGMENT

I would like to take this opportunity to show my deep appreciation to all the people who gave me help in the completion of this research about social media privacy and user awareness.

I would like to thank all the people who have participated in the survey by filling up the questionnaire. Their kind cooperation and honest responses are highly appreciated and will help me to get sufficient information to complete this research.

I would like to show my appreciation to my colleagues & friends for their continuous support, motivation and understanding during this research.

I would also like to thank all online resources and platforms that gave me useful references and information which helped in the completion of this research.

This paper could not have been completed without the help and cooperation of all the above-mentioned.

REFERENCES

[1]. https://blogs.infosys.com/emerging-technology-solutions/iedps/data-privacy-in-social-media-platforms-what-you-need-to-know.html
[2]. https://privsec.harvard.edu/best-practices-social-media
[3]. https://www.nicybersecuritycentre.gov.uk/social-media-how-secure-your-accounts
[4]. https://www.facebook.com/help/325807937506242/
[5]. https://help.instagram.com/196883487377501
[6]. https://www.linkedin.com/help/linkedin/answer/a1337839/?lang=en