

Data Privacy and Security in Social Media

Vardhan Janardhan Sadula¹, Aarti Sanjay Gawai²

¹ Student, Department of Information Technology and Computer Science, D.G. Ruparel College,

² Assistant Professor, Department of Information Technology and Computer Science, D.G. Ruparel College, Mumbai, Maharashtra, India

¹sadulavardhan28@gmail.com,² aartigawai1611@gmail.com

Abstract - Social media platforms such as Instagram, TikTok, X, and Snapchat have become an integral part of daily communication and content consumption. However, the extensive collection, processing, and sharing of users' personal and behavioural data have created significant privacy and security concerns. This study examines ten influential research papers on social media privacy and security to identify major developments, existing risks, and research gaps in the field. The review indicates that earlier studies primarily focused on conventional privacy risks, data disclosure, surveillance, and user awareness, while emerging threats such as AI-generated deepfakes, dark patterns, cross-platform tracking, and advanced behavioural profiling require greater attention. To address these gaps, this study proposes a conceptual framework called Smart-Shield Social (ZTFSA), designed to strengthen user privacy while supporting secure identity verification and personalized social media experiences. The framework incorporates privacy-preserving cryptographic mechanisms to minimise unnecessary exposure of users' personal information. The study concludes that stronger privacy-by-design approaches, transparent data practices, and user-centric security mechanisms are essential for creating safer and more trustworthy social media environments.

Key Words: Data Privacy, Social Media Security, User Privacy, AI Deepfakes, Dark Patterns, Online Tracking, Cryptography, Privacy by Design, Smart-Shield Social, ZTFSA

1. INTRODUCTION

In the digital era, social media has completely changed the way people communicate, share information, and stay connected with others. Platforms such as Facebook, Instagram, X (formerly Twitter), TikTok, and Snapchat have become an important part of everyday life. People use these platforms not only to communicate with friends and family but also to learn new things, follow current events, promote businesses, build professional networks, and express their opinions. Social media has made communication faster and easier, allowing people from different parts of the world to interact within seconds. However, along with these benefits, the growing use of social media has also created serious concerns related to data privacy and security.

Whenever a person uses a social media platform, a large amount of information is generated. This may include names, photographs, contact details, locations, search history,

messages, likes, comments, interests, and browsing behaviour. Even simple activities such as watching a video, liking a post, following an account, or clicking on an advertisement can provide information about a user's interests and preferences. Social media companies use this information to improve their services, personalize content, and show targeted advertisements. In some cases, information may also be shared with third parties for business and analytical purposes. The major concern is that many users do not fully understand what information is being collected, how long it is stored, or how it may be used. As a result, users may unknowingly give away more personal information than they intended.

Another major concern is the increasing number of online security threats. Social media accounts can become targets for phishing, hacking, identity theft, fake profiles, scams, malware, and unauthorized access. Cybercriminals often use information available on social media to make their attacks appear more convincing. For example, a person may receive a fake message that looks like it comes from a friend, bank, or well-known organization and may be tricked into sharing passwords or financial information. The problem has become even more complicated with the development of artificial intelligence. AI-generated content, deepfakes, and realistic fake profiles can make it difficult for users to distinguish between genuine and manipulated information. These developments show that protecting personal information requires more than simply using basic privacy settings.

At the same time, privacy is not only the responsibility of social media companies. Users also play an important role in protecting their own information. Simple practices such as using strong and unique passwords, enabling two-factor authentication, checking privacy settings, avoiding suspicious links, limiting unnecessary personal information, and being careful about accepting unknown friend or follower requests can significantly reduce online risks. However, many users either do not know about these practices or do not pay enough attention to them. This highlights the importance of digital literacy and awareness. Users need to understand that once personal information is shared online, it may be difficult to completely control where it goes or how it is used.

Therefore, data privacy and security on social media have become important issues for individuals, organizations, technology companies, and governments. There is a need for greater transparency about data collection and stronger security measures to protect users from unauthorized access and misuse of information. At the same time, users should be encouraged to make responsible decisions about what they share online. Finding the right balance between enjoying the benefits of social media and protecting personal privacy is a growing challenge in today's connected world.



2. Literature Review

Kumaraguru and Sachdeva (2014) conducted a large-scale study on privacy perceptions among Indian citizens. The researchers surveyed 10,427 people to understand their attitudes and awareness regarding privacy on mobile phones, online social networks and government platforms. The study found that Indian users considered financial information to be highly personal and were concerned about the possibility of third parties accessing their information. It also found that women were slightly more conscious about privacy than men. The study highlights the importance of increasing privacy awareness among Indian social media users.

Adhikari and Panda (2018) studied information privacy concerns and privacy-protection behaviour among social network users in India. The study used responses from 337 university students, of which 306 were included in the analysis. The findings showed that users who felt more vulnerable to privacy threats and believed that the consequences of data misuse could be serious were more concerned about their privacy. These privacy concerns were also significantly related to privacy-protection behaviour. The study suggests that users who understand the risks of sharing personal information are more likely to take steps to protect themselves online.

Pandey and Gudipudi (2018) examined the meaning of privacy from the perspective of Indian millennials using Facebook. The study found that Indian millennials considered sharing information such as their home address, mobile number, email address and purchasing preferences with third parties to be an invasion of privacy. However, the study also highlighted that users continue to share information on social media because of the benefits and convenience of these platforms. This study shows that there can be a difference between what users consider private and what they actually share online.

Bhandari, Bansal, Mathur and Nain (2022) examined privacy concerns and information-sharing behaviour among urban and rural social media users in India. The study also considered differences in privacy concerns among users with different levels of internet addiction. The researchers found that users' privacy concerns and information-sharing behaviour could vary according to their background and online behaviour. The study also indicated that many respondents were vulnerable to privacy infringement because of insufficient awareness about social media privacy.

Srivastava and Roychoudhury (2021) examined the factors that influence the adoption of privacy-protection features among Indian social network users. Using an online questionnaire, the

researchers collected responses from 392 Indian users. The study found that users' experiences with social networking and their privacy-related concerns influenced their use of privacy-protection features. The researchers emphasized that users need to understand how their information is shared and should be provided with simple and effective privacy controls.

The above Indian studies show that privacy awareness, privacy concerns, information-sharing behaviour and the use of privacy settings are important factors in protecting personal information on social media. However, there is still a need to understand how users currently deal with issues such as third-party data sharing, unauthorized access, phishing, account security and the protection of personal information. Therefore, the present study focuses on understanding the awareness, perceptions and security practices of Indian social media users regarding data privacy and security

3. Research Methodology

The study on "Data Privacy and Security in Social Media" follows a descriptive research design to understand users' awareness, concerns and practices related to protecting their personal information online. The study uses both primary and secondary data. Primary data is collected through a structured questionnaire from social media users, while secondary data is collected from research papers, journals, articles and reliable online sources. Convenience sampling is used to select the respondents, with a total sample size of [insert number] respondents. The collected data is analyzed using percentages, tables and charts to understand users' privacy awareness, information-sharing habits, use of privacy settings and security practices. The study mainly focuses on data privacy, security risks and personal-data protection on social media. However, the findings may be limited due to the sample size and the use of convenience sampling.

3.1 Research Design

The present study on "Data Privacy and Security in Social Media" follows a descriptive research design. The main purpose of the study is to understand how social media users are aware of privacy and security issues and how they protect their personal information while using social media platforms. The study focuses on users' daily experiences, their privacy concerns, and the security practices they follow. A descriptive approach is suitable because it helps present the current situation based on the responses collected from the participants.

3.2 Sources of Data

The study uses both primary and secondary data. Primary data is collected directly from social media users through a structured questionnaire. The questionnaire includes simple questions related to privacy awareness, sharing of personal information, privacy settings, security practices and common online threats. Secondary data is collected from research papers, academic journals, articles, reports and reliable online sources related to social media privacy and security. Both sources help in developing a better understanding of the research topic.

3.3 Sampling Method and Sample Size

For this study, convenience sampling is used to collect responses from people who regularly use social media platforms such as Instagram, Facebook, WhatsApp, YouTube and X. The respondents are selected based on their availability and willingness to participate in the survey. The questionnaire is shared online to make it easier for respondents to provide their

answers. The total sample size of the study is insert number respondents. The responses collected from these participants are used for further analysis and interpretation.

3.4 Data Collection and Analysis

The primary data is collected using a structured questionnaire prepared according to the objectives of the study. The questions mainly focus on users' awareness of data privacy, the type of personal information they share, their use of privacy settings, awareness of data collection, security practices and experiences with suspicious links or messages. After collecting the responses, the data is organized and analyzed using frequency, percentage, tables and charts. The results are then interpreted in simple terms to understand the general privacy and security behaviour of the respondents.

3.5 Scope and Limitations of the Study

The study mainly focuses on understanding data privacy and security among social media users. It covers important areas such as personal information sharing, privacy settings, data collection, third-party access, account security and awareness of common online threats. The study also aims to understand whether users take basic steps to protect their information while using social media. However, the study has some limitations. The sample size is limited, and convenience sampling may not represent the views of all social media users. The study is also based partly on the respondents' own answers, so their responses may differ from their actual online behaviour. Despite these limitations, the study provides a useful overview of users' awareness and practices related to data privacy and security on social media.

4. Data Privacy in Social Media

Data privacy in social media means protecting users' personal information such as photos, contact details, location and online activities. Social media platforms collect and use this data for different purposes, but users may not always know how their information is being used or shared. Poor privacy practices can lead to data misuse, identity theft, tracking and fraud. Therefore, users should be aware of privacy settings and avoid sharing sensitive personal information. They should also regularly review their account settings, use strong passwords and be careful about the information they make publicly available.

4.1 Collection of Personal Data

Social media platforms collect different types of personal information when people use their services. This may include names, phone numbers, photos, location, interests, search history and online activities. Most users share some of this information while creating accounts or using different features. However, many users may not fully understand how much data is being collected or how it is being used.

4.2 Privacy Settings and User Awareness

Privacy settings allow users to control who can see their posts, photos and other personal information. However, many users do not regularly check or update these settings. Some users may also accept the default settings without knowing what they allow. Therefore, creating awareness about privacy settings is important so that users can make better decisions about what they share online.

4.3 Risks of Data Privacy

Poor data privacy can create several risks for social media users. Personal information can be misused for identity theft, fraud, unwanted advertising, tracking or unauthorized access. Sharing too much information publicly can also make users more vulnerable to scams and cyber threats. Therefore, users should avoid sharing sensitive information and should regularly review their privacy and security settings.

4.4 Third-Party Data Sharing

Social media platforms may share or provide access to user information to third-party companies, advertisers, analytics providers, and other service providers. This information can be used to understand user interests, improve services, or provide personalized advertisements. For example, a user's online activities and preferences may be used to show advertisements related to products they have recently searched for or viewed. While such practices can make online services more personalized, they can also create privacy concerns when users are not clearly aware of how their information is being shared or used. Therefore, social media platforms should be more transparent about third-party data sharing and give users clear choices about how their personal information is handled.

4.5 Importance of Protecting Personal Data

Protecting personal data is important because information shared on social media can have a long-term impact on a person's privacy and safety. Users should think carefully before sharing sensitive details such as phone numbers, home addresses, financial information, passwords, travel plans, or personal documents online. Simple steps such as using strong passwords, enabling two-factor authentication, limiting the amount of personal information shared publicly, and checking privacy settings regularly can help reduce the risk of data misuse. At the same time, social media companies should take responsibility for protecting user information through strong security measures and clear privacy policies. When both users and platforms take privacy seriously, social media can become a safer and more trustworthy environment.

5. Data Security in Social Media

Data security in social media means protecting users' accounts and personal information from unauthorized access, hacking, phishing, scams and other online threats. Using strong passwords, two-factor authentication and secure login methods can help keep accounts safe. Users should also avoid suspicious links, unknown accounts and sharing sensitive information such as passwords and OTPs. Being aware and following basic security practices can reduce the chances of data theft and account misuse.

5.1 Account Security

Data security starts with protecting social media accounts from unauthorized access. Users should create strong and unique passwords and enable two-factor authentication (2FA) wherever possible. Regularly updating passwords and checking login activity can also help users identify unusual activity and keep their accounts safe.

5.2 Common Security Threats

Social media users face different security threats such as phishing, hacking, fake accounts, malware, scams and identity theft. Users may receive suspicious messages or links that appear genuine but are designed to steal passwords or personal information. Being careful about unknown accounts, links and messages can help reduce these risks.

5.3 Safe Security Practices

Good security practices can make social media use much safer. Users should avoid sharing passwords, OTPs and sensitive personal information with others. They should also review their account settings, use secure passwords and avoid clicking on suspicious links. Staying aware of common online threats helps users protect their accounts and personal data.

5.4 Role of Software Updates and Security Tools

Keeping social media apps and devices updated is an important part of maintaining data security. Updates often include security improvements that help protect users from newly discovered threats and weaknesses. Users should regularly update their mobile operating systems, social media applications, browsers, and security software instead of ignoring update notifications. Using trusted antivirus or security tools can also provide an additional layer of protection. These simple steps may seem small, but they can reduce the chances of attackers taking advantage of outdated software.

5.5 User Responsibility and Security Awareness

Users have an important role to play in keeping their social media accounts secure. Even when social media companies provide strong security features, careless online behaviour can still put personal information at risk. Users should be aware of suspicious messages, fake offers, unusual login alerts, and requests for passwords or OTPs. They should also avoid logging into accounts through unknown links or unsecured devices. Developing good digital habits and staying informed about new types of cyber threats can help users respond more safely when something unusual happens. Therefore, security awareness, along with responsible online behaviour, is essential for protecting social media accounts and personal information.

6. Common Security Threats in Social Media

Social media users face several security threats such as phishing, hacking, fake accounts, malware, identity theft, and online scams. Attackers often use fake links, messages, emails, or profiles that look genuine to trick users into sharing their passwords, personal details, bank information, or one-time passwords (OTPs). Sometimes, users may click on a suspicious link without realizing that it can install harmful software or take them to a fake website. Fake accounts can also be used to gain a person's trust and misuse their photos or personal information.

These threats can lead to account hacking, financial loss, privacy violations, and misuse of personal data. In some cases, attackers may even use stolen accounts to contact the victim's friends and family and ask for money. Many users become victims because they trust messages that appear to come from friends, companies, or other familiar sources. Therefore, users should think carefully before clicking unknown links, accepting requests from strangers, or sharing personal information online.



6.1 Phishing

Phishing is one of the most common security threats on social media. Attackers send fake messages, emails or links that look genuine and try to convince users to share their passwords, OTPs or other personal information. These messages may appear to come from friends, companies or trusted organizations. Users should always check the source before clicking on unknown links or sharing any information.

6.2 Hacking

Hacking occurs when someone gains unauthorized access to a social media account. Hackers may steal login details, change passwords, misuse personal information or even use the account to contact other people. Weak passwords and reused passwords can increase this risk. Using strong and unique passwords and enabling two-factor authentication can provide better protection.

6.3 Fake Accounts

Fake accounts are created by people who pretend to be someone else. These accounts may be used to spread false information, contact users with dishonest intentions or collect personal information. Sometimes, fake profiles are also used to cheat people or promote fraudulent activities. Users should carefully check profiles before accepting requests or sharing personal information.

6.4 Malware

Malware refers to harmful software that can enter a device through suspicious links, files or downloads shared on social media. Once installed, it can damage the device or allow attackers to access personal information. Users should avoid downloading files from unknown sources and should not click on suspicious links received through social media.

6.5 Identity Theft and Scams

Identity theft happens when someone steals personal information and uses it to pretend to be another person or commit fraud. Social media scams can also involve fake offers, prizes, job opportunities or requests for money and personal details. Users should be careful about what information they share online and should verify unusual requests before responding.

7. User Awareness of Data Privacy and Security in Social Media

User awareness is important for protecting personal information on social media. Users should know what data they share and how it may be collected and used.

They should regularly check and update their privacy settings. Awareness of phishing, fake accounts, scams, and hacking can prevent security risks. Using strong passwords and two-factor authentication improves account security. Users should avoid sharing sensitive personal information publicly. Therefore, better awareness can help users use social media safely and responsibly

7.1 Awareness of Personal Data Collection

Social media users share a large amount of personal information while creating accounts and using different platforms. This information may include names, photographs, phone numbers, email addresses, location, interests, contacts, and online activities. However, many users are not fully aware of how much information is collected and how it may be used. Some users believe that the information they provide is only visible to their friends, while in reality, certain information may also be collected and processed by the platform or third-party services. Therefore, awareness of personal data collection is an important part of responsible social-media usage. Users who understand what information is being collected are more likely to make careful decisions about what they share online.

7.2 Awareness of Privacy Settings

Privacy settings are important tools that allow users to control who can access or view their personal information. Social media platforms generally provide options to manage profile visibility, posts, photographs, location sharing, tagging, contact information, and other personal details. However, simply having privacy settings does not guarantee that users are protected. Many users do not regularly check or update these settings because they are unaware of their importance or find the options complicated. Users should therefore be encouraged to review their privacy settings regularly and limit access to their information wherever possible. Greater awareness of privacy controls can help users reduce unnecessary exposure of their personal information.

7.3 Awareness of Social Media Security Threats

Social media users face several security threats, including phishing, fake accounts, identity theft, hacking, scams, malware, and social engineering attacks. Attackers may create fake profiles or send attractive messages and links to convince users to reveal passwords, financial information, or other sensitive details. Users who are not familiar with these threats can easily become victims. Awareness plays an important role in preventing such incidents. Users should learn how to identify suspicious profiles, unknown links, unusual messages, and requests for personal information. They should also avoid sharing passwords or sensitive information through social-media messages.

7.4 Awareness of Safe Online Behaviour

Safe online behaviour is an important part of protecting privacy and security on social media. Users should think carefully before posting personal information, photographs, travel plans, addresses, financial details, or other sensitive content. Using strong and unique passwords, enabling two-factor authentication, logging out from shared devices, and avoiding suspicious links can provide additional protection. Users should also be careful when connecting third-party applications to their social-media accounts. Developing these habits can reduce the possibility of privacy violations and security

incidents. Thus, awareness should not only mean knowing about risks but also applying safe practices while using social-media platforms.

7.5 Importance of Privacy and Security Awareness

User awareness is one of the most important factors in protecting personal information on social media. Even when social-media companies provide privacy controls and security features, users also have a responsibility to use these tools properly. A lack of awareness can result in oversharing, weak passwords, acceptance of unknown requests, and exposure to online scams. On the other hand, informed users are more likely to understand privacy risks, control their information, identify suspicious activities, and use available security features. Therefore, increasing awareness through digital-literacy programmes, educational campaigns, clear privacy policies, and simple security guidance can help create safer social-media environments. User awareness should be considered an essential part of data privacy and security because technology alone cannot completely protect users from online risks.

7.6 Role of Education and Digital Awareness

Education plays an important role in improving users' understanding of data privacy and security. Social media users should be educated about privacy settings, online scams, phishing, fake accounts, password protection, and safe information sharing. Awareness programmes and digital literacy can help users identify online risks and make responsible decisions. Regular awareness campaigns can also encourage users to update their security settings and follow safe online practices. Schools, colleges, workplaces, and social media platforms can play an important role in providing privacy and security education. Users should also be encouraged to read privacy policies and understand how their personal information is collected and used. Learning about new online threats is important because cybercriminals continuously develop new methods to target users. Greater awareness can reduce careless sharing of personal information and improve users' confidence in protecting their online accounts..

8. CONCLUSIONS

Social media has become an important part of everyday life, helping people communicate, share information, build relationships, learn new things, and stay connected with the world. However, the increasing use of social media has also created serious concerns about data privacy and security. Users share a large amount of personal information such as photos, contact details, locations, interests, opinions, and online activities, often without fully understanding how this information is collected, stored, used, and shared. Security threats such as phishing, hacking, fake accounts, malware, identity theft, scams, and unauthorized access can further increase these risks. This study shows that protecting personal information is not only the responsibility of social media companies but also of individual users. Users need to understand privacy settings, create strong and unique passwords, enable two-factor authentication, avoid suspicious links, and think carefully before sharing sensitive information online. At the same time, social media platforms should follow strong security practices, provide clear privacy policies, protect user data, and make privacy controls simple and easy to understand.

Another important finding is that awareness plays a major role in improving data privacy and security. Many users accept

privacy policies, click on links, or share personal information without considering the possible consequences. This can happen because privacy and security information is often difficult to understand or users may not be aware of common online threats. Therefore, digital literacy and regular awareness programmes are important for helping people recognize phishing attempts, fake profiles, online scams, and other security risks. Educational institutions, organizations, governments, and social media platforms can work together to create greater awareness and encourage responsible online behaviour. Users should also develop the habit of checking their privacy settings regularly and being more careful about the information they make publicly available.

REFERENCES

1. Adhikari, K., & Panda, R. K. (2018). *Users' information privacy concerns and privacy protection behaviors in social networks*. Journal of Global Marketing, 31(2), 96–110.
2. Bhandari, M., Bansal, G., Mathur, S., & Nain, K. (2022). *Privacy concerns and information-sharing behaviour among social media users in India*.
3. Kumaraguru, P., & Sachdeva, S. (2014). *Privacy perceptions among Indian citizens: A study of privacy awareness and concerns in digital platforms*.
4. Pandey, S., & Gudipudi, A. (2018). *Understanding "What is Privacy" for Millennials on Facebook in India*.
5. Srivastava, D. K., & Roychoudhury, B. (2021). *Understanding the factors that influence adoption of privacy protection features in online social networks*.
6. Jain, A. K., Sahoo, S. R., & Kaubiyal, J. (2021). *Online social networks security and privacy: Comprehensive review and analysis*. Complex & Intelligent Systems, 7, 2157–2177.
7. Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). *Privacy and human behavior in the age of information*. Science, 347(6221), 509–514.
8. Krombholz, K., Merkl, D., & Weippl, E. (2015). *Fake identities in social media: A case study on the sustainability of online identity*. International Journal of Information Security.
9. Krombholz, K., Merkl, D., & Weippl, E. (2015). *Fake identities in social media: A case study on the sustainability of online identity*. International Journal of Information Security, 14, 479–492.
10. Kayes, I., & Iamnitchi, A. (2015). *Privacy and security in online social networks: A survey*. Online Social Networks and Media, 3–4, 1–21.
11. Taddicken, M. (2014). *The "privacy paradox" in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure*. Journal of Computer-Mediated Communication, 19(2), 248–273.
12. Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). *Online social networks: Why we disclose*. Journal of Information Technology, 25(2), 109–125.
13. Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). *Privacy and human behavior in the age of information*. Science, 347(6221), 509–514.
14. Dienlin, T., & Trepte, S. (2015). *Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors*. European Journal of Social Psychology, 45(3), 285–297.
15. Chen, H., & Chen, W. (2015). *The privacy paradox and social media: A systematic review of privacy concerns and disclosure behaviour*. Social Media + Society.

BIOGRAPHIES



Mr. Vardhan Janardhan Sadula
Student of M.Sc Information
Technology Dept.
D.G Ruparel College



Ms. Aarti Sanjay Gawai
M.Sc Information Technology
Asst. Prof.IT/CS Dept.
D.G Ruparel College