International Journal of Scientific Research and Engineering Development-– Volume 9 Issue 1, Jan-Feb 2026
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Data Privacy Concerns in Social Media Applications

Mrs Deepa V[1], Ms Vismaya Prasanth[2]
[1]Assistant Professor, Department of Computer Science, Sri Ramakrishna College of Arts & Science, Coimbatore.
[2]III B.Com CA, Sri Ramakrishna College of Arts & Science, Coimbatore.

1.ABSTRACT

Social media applications have become an indispensable channel for communication in this contemporary era, while at the same time giving rise to major concerns related to the privacy and security of user information. This paper focuses on the major data privacy issues in popular social media applications: Facebook, Instagram, Snapchat, X, and TikTok. It examines how these social media applications collect, store, and use personal data, reviewing the existing research on the privacy risks, data misuse, user awareness, and regulatory frameworks like GDPR. The study concludes that despite social media platforms offering various advanced tools to enhance their security, users continue to pose a threat to their privacy because of weak awareness, excessive data sharing, algorithmic tracking, and third-party access.

2.INTRODUCTION

The research focuses on the concern for data privacy related to popular social media sites such as Facebook, Instagram, TikTok, Snapchat, and X, in the context of modern-day communication. These sites allow people from around the world to connect, share information, express opinions, and engage in social and entertainment activities, and as a result, a large amount of personal and behavioral data is created every day.

Despite their benefits, social media sites also raise important issues of privacy and security. Users tend to share their personal information, including photos, contact information, location, and activities, without fully understanding the implications of such information being collected, stored, and processed. A large amount of information is also processed using algorithms for advertising and analytics purposes, often using third-party apps. The risks associated with privacy have escalated because of constant tracking of user behavior, the lack of proper default privacy settings, and unauthorized use of personal data. There have been many cases of data breaches and misuse that have highlighted the susceptibility of user data on such platforms. Also, the privacy policies are usually complex and difficult to understand.

Despite the availability of privacy controls and security measures offered by social media platforms, users often remain unaware of these options or neglect to set them up properly. This is despite the presence of regulatory measures such as the General Data Protection Regulation (GDPR) in the European Union and the Digital Personal Data Protection (DPDP) Act in India, which are designed to protect the data of social media users.

The current review integrates the key issues regarding data privacy that are linked with popular social media applications by reviewing the existing literature. Additionally, this review proposes an algorithmic approach for assessing the privacy risk and underlines the importance of increased transparency, stronger regulations, and greater awareness for ensuring data privacy in the context of social media.

3.REVIEW OF LITERATURE

1. Mitchell & El-Gayar 2022

Title: Privacy and Online Social Networks: A Systematic Literature Review of Concerns, Preservation, and Policies

In this paper, Mitchell and El-Gayar examine the notion of privacy concerns among users of social media sites. According to them, identity theft, unauthorized data sharing, and poor clarity of privacy tools are considered as the three major threats. The authors also observe that users often do not know how to properly set privacy settings.

Link: https://aisel.aisnet.org/pajais/vol14/iss4/1/

2.Hassan, Siddiqua & Ayaz (2024)

Title: Critical Analysis of the Ethical Challenges Related to Data Privacy and Social Media Analytics

This review analysis, based on 38 research articles, identifies a lack of transparency regarding data handling by the social media companies. Users often consent to a long, complicated privacy policy without full comprehension and may consequently share more data than they intended.

Link: https://www.gmcrjournal.com/article/critical-analysis-of-the-ethical-challenges-related-to-data-privacy-and-social-media-analytics-a-literature-review

3. Krasnova et al. (2009)

Title: Privacy Concerns and Identity within Online Social Networks

Krasnova et al. show that privacy concerns affect online disclosure, modulating how much information a user discloses because of organizational threats (misuse by companies) or social threats (misuse by other users).

Link: https://philpapers.org/rec/KRAPCA

4. Information Privacy in Online Social Networks (2018)

Title: Information Privacy in Online Social Networks: Uses and Gratifications Perspective

This study demonstrates that users continue sharing personal information despite privacy risks because perceived benefits such as social interaction and entertainment outweigh the risks.

Link:https://www.sciencedirect.com/science/article/pii/S0747563218301213 2.5

5. The Social Network Dilemma (2024)

Title: The Social Network Dilemma: Safeguarding Privacy and Security in an Online Community

This open-access review highlights privacy and security challenges in online social networks, including data breaches, identity theft, and cyberstalking. It also reviews security measures (e.g., encryption, authentication) and calls for transparent data protection policies and user empowerment to enhance privacy outcomes.

Link: https://iieta.org/journals/ijsse/paper/10.18280/ijsse.140112

4. OBJECTIVES

1. Identify major data privacy concerns within social media applications.
2. Assess user awareness about privacy risks.
3. Look at how the platforms gather and process information from their users.
4. Review the existing scholarly literature on privacy issues and ethical challenges.
5. Suggest ways to increase data protection.

5. METHODOLOGY

This research uses secondary data obtained from scholarly articles and other academic works covering the period 2009 to 2025. It focuses on the aspects of privacy risks, user behavior, and ethical considerations concerning social media sites.

Algorithm: Privacy risk assessment in social media applications

Objective: Identify and assess the privacy risks associated with user data shared on social media platforms.

Input: User profile data will include but are not limited to the following: name, email, posts, photos, location.

- User account privacy settings
- Inventory of connected third-party applications

Steps:

- **Data Collection**
  - Collect personal information, posts, photos and videos

- Identify connected applications and corresponding permissions

- **Data Classification**
  - PII: name, phone number, email
    Sensitive data: location, Private photos of health information
  - Behavioral data: likes, posts, browsing patterns
- **Privacy Setting Analysis**
  - Classify the visibility of each data item: Public, Friends Only, Private
- **Third-Party Access Assessment**
  - Identify applications authorised to access user data
  - Evaluate the kind and amount of data available for each application

Set Privacy Risk Scores:
High risk → sensitive public data
Low risk → completely private
Medium risk → shared with friends create a privacy report by listing every data item along with its risk score. Make charts that display the percentages of high, medium, and low-risk data as an optional visualization.
Output:
- Each user profile's privacy risk report
- Suggestions for enhancing privacy

6. FINDINGS AND DISCUSSIONS

The findings emerging from algorithmic analysis and the existing literature suggest that there are a number of prominent privacy issues associated with social media applications. Firstly, there is an overreliance on data collection, which often sees applications collect significantly more information than users are aware of. At the same time, there is a lack of awareness regarding privacy policies and security settings, which are often not fully comprehended by users. Moreover, there is a significant amount of third-party data sharing, which sees a number of applications access and share sensitive user information without the users' awareness. At the same time, behavioral aspects also contribute to the problem, as users often opt to use the social benefits of applications despite potential privacy issues. Moreover, there are also significant security risks associated with social media applications, including data breaches and phishing attacks, which pose a significant threat to data protection. Taken together, these points highlight the need for more stringent regulations, emphasizing that the GDPR, India's Digital Personal Data Protection (DPDP) Act, and similar regulations are long overdue.

7. CONCLUSION

Social media applications provide a useful means of communication and entertainment, but they also expose users to some significant privacy risks. The literature suggests that there is a general lack of awareness by users, that the policies are often unclear, and privacy protections are seriously inadequate. The algorithm developed here offers a systematic way to review and report on privacy risks associated with user data. For future work, it is recommended to focus more on enhanced transparency, regulatory enforcement, and user education about privacy protection.

8. REFERENCES

1. **Mitchell, D. R., & El-Gayar, O. F. (2022).** Privacy and online social networks: A systematic literature review of concerns, preservation, and policies. Retrieved from https://aisel.aisnet.org/pajais/vol14/iss4/1/
2. **Hassan, K., Siddiqua, A., & Ayaz, W. B. (2024).** Critical analysis of the ethical challenges associated with data privacy and social media analytics. Retrieved from https://www.gmcrjournal.com/article/critical-analysis-of-the-ethical-challenges-related-to-data-privacy-and-social-media-analytics-a-literature-review

3. **Krasnova, H., Günther, O., Spiekermann, S. & Koroleva, K. (2009).** Privacy concerns and identity in online social networks. Retrieved from https://philpapers.org/rec/KRAPCA
4. **Information privacy in online social networks: Uses and gratification perspective. (2018).** Retrieved from https://www.sciencedirect.com/science/article/pii/S0747563218301213
5. **The Social Network Dilemma: Safeguarding Privacy and Security in an Online Community. (2024).** International Journal of Social Sciences and Economics (IJET). Retrieved from https://iieta.org/journals/ijsse/paper/10.18280/ijsse.140112

