

ONLINE PRIVACY AWARENESS AMONG SOCIAL MEDIA USERS

Dr. Divya Bansal

Professor & Head

Department of Computer Science and Engineering
Punjab Engineering College (Deemed to be University)
Chandigarh, India

Abstract

Social media platforms enable users to communicate, build communities, obtain information, promote work, and participate in public discussion. At the same time, ordinary activities such as posting, reacting, tagging, following, granting app permissions, and accepting platform defaults can create privacy risks. Users may reveal personal, relational, behavioural, and location-linked information without fully understanding who can access it, how long it can persist, or how it can be used for profiling, advertising, fraud, or reputational assessment. Online privacy awareness therefore involves more than knowing that privacy settings exist; it requires the ability to recognise data flows, assess audiences, anticipate consequences, and make informed choices about disclosure.

This study examines online privacy awareness among social media users through an evidence-informed conceptual and comparative approach. It analyses five connected dimensions: privacy literacy, account and audience configuration, disclosure and digital-footprint management, permissions and third-party data sharing, and recognition of scams, impersonation, and manipulative design. Particular attention is given to the difference between users' general concern about privacy and their actual protective practices. The paper considers how platform complexity, peer expectations, convenience, information overload, and unequal digital skills can influence privacy decisions across different user groups.

The analysis indicates that privacy awareness is most effective when users receive clear, practical, and context-specific support rather than abstract warnings alone. Accessible privacy controls, safer defaults, two-factor authentication, audience review, permission checks, digital-literacy education, and transparent platform communication can reduce avoidable exposure. The study concludes that online privacy should be treated as a shared responsibility involving users, platforms, educators, policymakers, and community networks. Inclusive privacy awareness initiatives can help social media users participate confidently while maintaining greater control over their personal information and online identities.

Keywords: Online Privacy, Social Media Users, Privacy Awareness, Digital Literacy, Data Protection, Privacy Settings, Digital Footprint, Account Security, Data Sharing, Platform Governance

1. INTRODUCTION

Social media has become a routine environment for interpersonal communication, learning, entertainment, professional networking, commerce, and public participation. Users create profiles, share images and messages, join groups, interact with brands, and connect with people across geographic boundaries. These activities can create social and economic value, but they also produce detailed digital traces. Profile information, content metadata, contact networks, browsing signals, device identifiers, and engagement patterns may reveal more about an individual than a single post appears

to disclose. Privacy awareness is therefore an essential component of responsible digital participation.

Online privacy in social media is not only a matter of secrecy. It concerns a person's ability to understand and influence how personal information is collected, interpreted, shared, retained, and repurposed in different contexts. A user may be comfortable sharing a photograph with close friends but not with employers, unknown contacts, automated recommendation systems, advertisers, or data brokers. This context-sensitive nature of privacy makes social media decisions difficult, especially when platform settings, policy

language, and data practices are complex or frequently changed.

Many privacy risks arise from ordinary decisions that appear convenient or harmless. Public accounts can expose content to unintended audiences; location tags can reveal routines; third-party applications can request broad permissions; and weak passwords can make accounts vulnerable to takeover. Users may also encounter phishing messages, impersonation, fraudulent offers, harassment, and social-engineering attempts that exploit personal information already visible online. Such risks are not distributed equally. People with limited digital literacy, new users, minors, older adults, public-facing professionals, and small-business operators may face different forms of vulnerability.

This paper explores how online privacy awareness can support safer social media use. It reviews key privacy concepts, identifies common risks and protective practices, presents a comparative framework for user contexts, and discusses how practical awareness measures can improve informed decision-making. The study does not claim to measure one specific platform or population; instead, it synthesises established privacy dimensions to show how awareness can be strengthened across diverse social media environments.

2. LITERATURE REVIEW

Privacy scholarship generally recognises that individuals do not make disclosure decisions in a purely rational or stable manner. Decisions are shaped by social expectations, perceived benefits, trust in platforms, interface design, past experience, available information, and the immediate context of sharing. In social media spaces, users often manage multiple audiences at once, including friends, family, classmates, colleagues, customers, and strangers. The collapse of these audiences can make it difficult to judge whether a post, profile field, or interaction is appropriate for all potential viewers.

Research also distinguishes between privacy concern, privacy literacy, and privacy-protective behaviour. A person may express concern about misuse of personal information while still using public settings, accepting permissions without review, or repeatedly disclosing sensitive details. This gap is often

described as the privacy paradox. It should not be interpreted as proof that users do not care about privacy; rather, it reflects the practical constraints of digital environments, including limited time, confusing notices, default settings, social pressure, and uncertainty about future consequences.

The literature further shows that privacy is influenced by technical and institutional conditions. Users can make better choices when controls are understandable, defaults are protective, requests for data are specific, and reporting pathways are available. However, individual action alone cannot address every risk. Platforms, developers, educators, regulators, and civil-society organisations also shape the privacy environment through design standards, transparency, accountability, education, and enforcement.

2.1 DIGITAL PRIVACY IN SOCIAL MEDIA ENVIRONMENTS

- Social media privacy includes control over profile information, content visibility, location data, contacts, behavioural data, and the reuse of information across contexts.
- A post can have multiple audiences beyond the intended recipient because screenshots, downloads, resharing, search functions, and recommendation systems may extend its reach.
- Platform data practices can involve the collection of interaction signals, device information, inferred interests, and audience data that users may not easily observe.
- Privacy risks can be personal, social, financial, and professional, including identity theft, fraud, discrimination, harassment, reputational harm, and unwanted surveillance.

2.2 PRIVACY AWARENESS, LITERACY, AND PROTECTIVE PRACTICES

- Privacy awareness includes understanding what information is sensitive, who may access it, how long it may remain available, and what risks can follow from disclosure.
- Privacy literacy helps users interpret settings, notices, permissions, audience controls, authentication options, and reporting tools in a practical way.

- Protective practices include limiting profile details, reviewing account visibility, using strong unique passwords, enabling multi-factor authentication, and checking connected applications.
- Effective awareness programmes should use realistic examples and simple actions because users are more likely to apply guidance that is directly connected to their daily social media routines.

2.3 PRIVACY PARADOX AND USER VULNERABILITIES

- Users may value privacy but still disclose information when sharing brings social connection, convenience, visibility, entertainment, or access to a desired service.
- Complex settings, lengthy privacy notices, interface nudges, and rapidly changing features can reduce a user's practical ability to make informed choices.
- Different users face different vulnerabilities: students may experience peer pressure, professionals may face reputational exposure, and older users may be targeted by fraud or impersonation.
- Privacy awareness should therefore be inclusive and avoid assuming that one type of message or one technical solution will work equally well for every user group.

2.4 PLATFORM DESIGN AND GOVERNANCE CHALLENGES

- Default visibility settings, recommendation features, data-sharing prompts, and targeted advertising systems can influence privacy outcomes before users actively make a choice.
- Transparent explanations, meaningful consent, plain-language controls, and timely security alerts can help users understand and manage data practices.
- Platform governance should include accessible reporting, account-recovery

support, safeguards against impersonation, and responses to abusive or fraudulent behaviour.

- Sustainable privacy protection requires coordination among users, platforms, schools, families, workplaces, consumer-protection agencies, and data-protection authorities.

3. OBJECT OF STUDY

The present study focuses on online privacy awareness among social media users. Its central purpose is to examine how awareness, digital literacy, privacy settings, disclosure behaviour, security practices, and platform design can reduce avoidable privacy risks while supporting meaningful online participation. The study treats privacy awareness as a practical capacity through which users recognise data-related risks, evaluate the likely audience and consequences of sharing, and choose suitable protective actions.

The analysis is conceptual and comparative. It does not report survey findings from one specific platform or population. Instead, it synthesises common privacy challenges and protective responses across representative user contexts. The framework is intended to assist researchers, educators, platform managers, community organisations, and users in identifying priority areas for privacy awareness and safer social media engagement.

3.1 THEORETICAL BASIS AND USER CONTEXTS CONSIDERED

From a privacy perspective, social media safety is shaped by the relationship between personal information, audience uncertainty, platform design, individual skills, social incentives, and institutional safeguards. The study considers representative user contexts to compare common forms of privacy exposure and the awareness practices that can help address them.

S. No.	User Profile	Typical Privacy Exposure	Awareness / Protection Practice	Key Significance
1	Everyday high-frequency user	Broad audience visibility, profile scraping, and persistent posts	Audience review, visibility controls, and careful sharing	Reduces unintended exposure
2	Student and young adult user	Peer pressure, location sharing, and third-party quizzes	Privacy literacy, permission checks, and digital-footprint review	Supports safer participation

3	Professional network user	Employment, reputation, and contact-data exposure	Separate audiences, profile minimisation, and account security	Protects identity and workplace boundaries
4	Creator or small-business operator	Public attention, impersonation, and customer-data misuse	Two-factor authentication, moderation, and role separation	Maintains trust and resilience
5	First-time or older user	Fraud, phishing, social engineering, and confusing defaults	Scam recognition, trusted support, and simple controls	Prevents financial and identity harm

3.2 STUDY OBJECTIVES

- To examine the relationship between social media use, online disclosure, and privacy awareness.
- To identify common privacy risks involving account visibility, personal data, third-party permissions, scams, and impersonation.
- To analyse the role of privacy literacy, account-security practices, and digital-footprint management in safer social media participation.
- To compare privacy-awareness priorities across representative social media user contexts.
- To develop an integrated conceptual framework for practical, inclusive, and user-centred privacy awareness.

4. RESEARCH METHODOLOGY

The study adopts a conceptual and comparative research methodology. It draws on established privacy scholarship, digital-literacy literature, platform-governance discussions, and data-protection principles to identify the conditions that influence privacy awareness in social media use. The methodology connects common privacy risks with practical user actions and institutional responsibilities rather than measuring the behaviour of a single platform or sample.

A qualitative framework is used to examine the interaction between disclosure choices, audience settings, security practices, platform interfaces, social expectations, and support systems. The analysis recognises that social media users differ in age, purpose of use, digital confidence, social networks, and exposure to risk. Privacy awareness should therefore be adapted to context while following shared principles of clarity,

informed choice, minimisation of exposure, security, inclusion, and accountability.

4.1 RESEARCH DESIGN

- The study follows an evidence-informed conceptual and comparative research design.
- Privacy risks are examined through the linked dimensions of data exposure, audience uncertainty, user capability, platform design, and protective response.
- The framework compares representative user contexts rather than generating platform-specific or population-specific statistical estimates.
- The analysis emphasises practical privacy awareness because risks often arise from a combination of user choices, social conditions, and technical settings.

4.2 ANALYTICAL FRAMEWORK

- Privacy literacy and contextual understanding of personal-information flows.
- Account settings, audience controls, password practices, and multi-factor authentication.
- Disclosure decisions, digital-footprint management, and separation of personal and professional identities.
- Permissions, connected applications, personalisation, advertising, and third-party data sharing.
- Scam recognition, reporting, platform support, public education, and accountability mechanisms.

4.3 PRIVACY AWARENESS INDICATORS

- Ability to identify sensitive profile details, location information, financial prompts, and content that may expose other people.

- Understanding of audience controls, search visibility, tagging approvals, direct-message settings, and account recovery options.
- Frequency of reviewing privacy settings, connected applications, device sessions, and permissions granted to external services.
- Use of strong unique passwords, multi-factor authentication, verification steps, and safe responses to suspicious messages.
- Awareness of data retention, screenshots, resharing, profiling, fraudulent contact, and the potential long-term effects of digital footprints.

4.4 PARAMETERS OF ANALYSIS

The analysis evaluates the following privacy-awareness parameters:

- Perceived control over personal information and understanding of the likely audience for content.
- Visibility of profiles, posts, location signals, contact lists, and other identifiers across social media settings.
- Security of accounts, devices, recovery channels, and authentication practices.
- Quality of decisions about personal disclosure, tagging, reposting, and sharing information about others.
- Ability to recognise deceptive messages, impersonation, social engineering, and unsafe third-party applications.
- Availability of clear controls, trusted guidance, reporting mechanisms, and accountable platform governance.

4.5 PROCEDURE OF STUDY

- Review privacy concepts, social media research, digital-literacy guidance, and data-protection principles.
- Identify recurring privacy risks associated with profiles, content sharing, account access, permissions, and deceptive contact.
- Organise protective responses into privacy literacy, settings, security, disclosure, support, and governance dimensions.
- Compare representative user contexts to identify context-specific awareness priorities.
- Interpret how individual practices and platform-level measures can reduce exposure and improve informed choice.
- Develop practical implications for privacy education, social media design,

community outreach, and responsible user participation.

4.6 ANALYTICAL APPROACH

- Qualitative comparison of common privacy risks and protective practices in social media environments.
- Assessment of interactions between user behaviour, social pressure, platform design, security features, and institutional support.
- Identification of co-benefits and limitations associated with privacy-awareness interventions.
- Use of an illustrative privacy-awareness matrix to demonstrate priority-setting for diverse social media users.

5. DATA ANALYSIS

The data analysis is based on a structured qualitative synthesis of the privacy dimensions identified in the literature. The purpose is not to claim that all users experience social media in the same way. Instead, the analysis demonstrates how privacy awareness can be interpreted through common questions: What information is being shared? Who can access it? What data may be inferred or reused? What technical controls are available? Which users may face greater difficulty in recognising or responding to risk?

The synthesis indicates that privacy awareness becomes stronger when information, settings, security practices, and support systems are considered together. A user who understands the risks of public posting may still be vulnerable if account recovery is weak, connected applications retain unnecessary permissions, or platform defaults are confusing. Similarly, a user who enables privacy settings may still experience harm if another person shares their image, impersonates their account, or uses visible information for fraud. Effective privacy protection therefore requires a combination of technical, behavioural, social, and institutional measures.

The comparative assessment also shows that no single warning message or privacy tool is sufficient. Privacy notices can improve understanding, but their effect may be limited when users face information overload or time pressure. Two-factor authentication can reduce account takeover, but it does not prevent oversharing or manipulative messages. User

education is important, but it should be supported by privacy-friendly defaults, clear interface design, transparent data practices, accessible reporting, and appropriate regulatory oversight.

5.1 ILLUSTRATIVE COMPARATIVE PRIVACY-AWARENESS ASSESSMENT

Table 2 presents an illustrative matrix for interpreting the contribution of selected

privacy-awareness measures. The classifications are conceptual and are intended to show relative priority rather than numerical performance values for a specific social media platform or user population.

Privacy Dimension	Typical User Risk	Priority Awareness Action	Expected Contribution
Account settings and audience control	Unintended public visibility and context collapse	Review profiles, post visibility, tagging, and search settings	High - limits accidental disclosure
Permissions and data sharing	Excessive access by apps, advertisers, or connected services	Check permissions, remove unused apps, and minimise data sharing	High - improves data control
Account security	Account takeover, impersonation, and loss of access	Use unique passwords, multi-factor authentication, and recovery safeguards	High - protects identity and contacts
Disclosure and digital footprint	Oversharing, reputational harm, and long-term content persistence	Assess audience, sensitivity, future impact, and information about others	Medium to high - supports informed sharing
Scams and platform support	Phishing, fraudulent contact, harassment, and weak reporting response	Recognise warning signs, verify requests, report abuse, and seek support	High - strengthens safe response

6. DISCUSSION

The analysis confirms that online privacy awareness should be understood as a continuing digital-life skill, not a one-time technical task. Social media practices change as users join new groups, begin employment, start a business, use a new device, or encounter new platform features. Privacy decisions also change when audience expectations, personal relationships, and public exposure change. Users need simple routines for reviewing settings, checking permissions, assessing suspicious contact, and reconsidering what they share.

One of the most important findings is the role of contextual disclosure. The same information can be appropriate in one setting and harmful in another. For example, a public professional profile may require a visible identity and contact channel, while a private personal account may require stronger audience limits and less personal detail. Awareness initiatives should help users distinguish between public, private, and mixed-audience contexts rather

than promoting an unrealistic expectation that every user should share nothing online.

Account security is another central component of privacy awareness. Weak or reused passwords, unprotected recovery emails, unrecognised device sessions, and responses to deceptive messages can lead to account takeover and broader exposure of personal contacts and content. Security guidance should therefore be integrated with privacy education. Users should understand how to enable multi-factor authentication, protect recovery channels, recognise phishing attempts, and seek help quickly when an account is compromised.

The discussion also highlights the importance of platform responsibility. Users cannot make meaningful choices when controls are hidden, terms are unclear, requests are framed manipulatively, or reporting systems are difficult to use. Platforms should reduce unnecessary collection, provide understandable controls, respect contextual audience choices, give clear notice of

significant changes, and maintain effective systems for reporting fraud, abuse, impersonation, and unauthorised access. Privacy-by-design practices can reduce the burden placed on individual users.

Finally, privacy awareness must address inclusion. Technical advice that assumes high literacy, secure devices, stable internet access, or familiarity with English-language interfaces may exclude many users. Guidance should be available in accessible language and local contexts, with examples relevant to students, workers, families, older adults, creators, and small businesses. A privacy-aware social media culture should support people in participating, learning, and communicating without making avoidable exposure a condition of digital inclusion.

7. CONCLUSION

This study presented a conceptual and comparative examination of online privacy awareness among social media users. The analysis showed that privacy awareness is shaped by the combined effect of user knowledge, disclosure choices, account settings, security practices, platform design, social context, and institutional safeguards. Users who lack clear information or practical

control may unintentionally expose personal information through public profiles, oversharing, weak account security, third-party permissions, or deceptive contact.

The study emphasises that privacy awareness should help users understand data flows, review audience settings, manage digital footprints, secure accounts, assess app permissions, and respond safely to suspicious messages. These actions can improve personal safety, reduce fraud and reputational harm, and support more confident participation in online communities. They are most effective when supported by understandable platform controls, privacy-friendly defaults, education, reporting pathways, and appropriate data-protection standards.

The paper concludes that social media privacy requires adaptable, practical, and inclusive awareness frameworks. Future work can apply the proposed framework to particular platforms or communities through surveys, interviews, usability assessments, digital-literacy interventions, and longitudinal studies of privacy behaviour. Such research can help translate broad privacy principles into accountable and user-centred practices for safer social media participation.

8. REFERENCES

1. Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221), 509-514. doi:10.1126/science.aaa1465
2. Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication*, 67(1), 26-53. doi:10.1111/jcom.12276
3. boyd, d., & Hargittai, E. (2010). Facebook privacy settings: Who cares? *First Monday*, 15(8). doi:10.5210/fm.v15i8.3086
4. Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, 15(1), 83-108. doi:10.1111/j.1083-6101.2009.01494.x
5. 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. doi:10.1002/ejsp.2049
6. Egelman, S., Tsai, J. Y., Cranor, L. F., & Acquisti, A. (2009). Timing is everything? The effects of timing and placement of online privacy indicators. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 319-328. doi:10.1145/1518701.1518752
7. European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). *Official Journal of the European Union*, L119, 1-88.
8. Federal Trade Commission. (2022). Bringing dark patterns to light: An FTC staff report. Federal Trade Commission, Washington, DC.
9. Government of India. (2023). Digital Personal Data Protection Act, 2023. *Gazette of India*, New Delhi.

10. Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, 71-80. doi:10.1145/1102199.1102214
11. Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 64, 122-134. doi:10.1016/j.cose.2015.07.002
12. Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology*, 25, 109-125. doi:10.1057/jit.2010.6
13. Livingstone, S. (2008). Taking risky opportunities in youthful content creation: Teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media & Society*, 10(3), 393-411. doi:10.1177/1461444808089415
14. Marwick, A. E., & boyd, d. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, 16(7), 1051-1067. doi:10.1177/1461444814543995
15. Masur, P. K. (2019). *Situational privacy and self-disclosure: Communication processes in online environments*. Springer.
16. National Institute of Standards and Technology. (2020). *NIST Privacy Framework: A tool for improving privacy through enterprise risk management, version 1.0*. NIST, Gaithersburg, MD.
17. Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, 79, 119-157.
18. OECD. (2013). *OECD guidelines governing the protection of privacy and transborder flows of personal data*. OECD Publishing, Paris.
19. Pew Research Center. (2019). *Americans and privacy: Concerned, confused and feeling lack of control over their personal information*. Pew Research Center, Washington, DC.
20. Schaub, F., Balebako, R., Durity, A. L., & Cranor, L. F. (2015). A design space for effective privacy notices. *Proceedings of the Eleventh Symposium on Usable Privacy and Security*, 1-17.
21. Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, 154(3), 477-560.
22. Stutzman, F., Capra, R., & Thompson, J. (2011). Factors mediating disclosure in social network sites. *Computers in Human Behavior*, 27(1), 590-598. doi:10.1016/j.chb.2010.10.017
23. 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 Consumer Policy*, 37, 249-273. doi:10.1007/s10603-014-9253-2
24. Trepte, S., & Reinecke, L. (Eds.). (2011). *Privacy online: Perspectives on privacy and self-disclosure in the social web*. Springer.
25. UNESCO. (2021). *Media and information literacy curriculum for educators and learners*. UNESCO, Paris.
26. Westin, A. F. (1967). *Privacy and freedom*. Atheneum, New York.
27. Wisniewski, P., Knijnenburg, B. P., & Lipford, H. R. (2017). Making privacy personal: Profiling social network users to inform privacy education. *Computers & Security*, 70, 116-130. doi:10.1016/j.cose.2017.06.006
28. Youn, S. (2005). Teenagers' perceptions of online privacy and coping behaviors: A risk-benefit appraisal approach. *Journal of Broadcasting & Electronic Media*, 49(1), 86-110. doi:10.1207/s15506878jobem4901_6
29. Bazarova, N. N., & Choi, Y. H. (2014). Self-disclosure in social media: Extending the functional approach to disclosure motivations and characteristics on social network sites. *Journal of Communication*, 64(4), 635-657. doi:10.1111/jcom.12106
30. Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy*, 3(1), 26-33. doi:10.1109/MSP.2005.22