International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

(REVIEW ARTICLE)

A Comprehensive Review of Data Privacy Challenges in Social Media Platforms

Manikantan R *, Meghana J and Padmavathi C

Department of MCA, Surana College (Autonomous), Bengaluru, India.

International Journal of Science and Research Archive, 2025, 17(01), 437-443

Publication history: Received on 02 September 2025; revised on 07 October 2025; accepted on 10 October 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.17.1.2795

Abstract

'Social media privacy has become one of the most urgent 21st-century digital concerns, as sites frame communication, identity, and public discourse while also facilitating surveillance, profiling, and exploitation. This review examines twenty peer-reviewed articles from 2003 to 2024, drawn from IEEE, Springer, ACM, and Scopus. The research was grouped into four broad categories: user behavior and awareness, legal and regulatory environment, risks and threats, and privacy enhancing technologies. The findings suggest that while technical solutions (e.g., encryption, differential privacy, federated learning) and policy tools (e.g., GDPR, CCPA, DPDP) are changing, they are not aligned with user understanding, cultural environments, and platform incentives. User literacy deficits, ineffective regulation, and data monetization-based business models remain eroding privacy protections. The review underscores the imperative for interdisciplinary approaches that merge legal, technical, and social insights, ensuring privacy-by-design systems that are easy to use and culturally sensitive.

Keywords: Privacy Risks and Challenges; User behavior and awareness; GDPR and Data Protection; Legal and Regulatory Frameworks; Social Media Platforms

1. Introduction

Social media is deeply integrated into daily life, facilitating communication, self expression, and collaboration across the globe. Concurrently, they provide unparalleled challenges to protecting user data. Social media privacy is complex because it results from intersecting factors—user behaviour, regulatory environments, technological protections, and commercial incentives—that are frequently at odds with each other. This review paper is framed by the following questions of investigation: What are the recurring themes in the literature on social media privacy? How do legal, technical, and user-oriented perspectives converge in solving privacy problems? What are the limitations and gaps of existing studies, and how can they be addressed in future studies? The contributions of this review are threefold: It integrates twenty years of research (2003–2024) by categorizing studies into four major categories: user awareness, legal frameworks, risks and threats, and privacy-preserving technologies. It offers comparative analysis of methodology, results, and limits in various geographical, cultural, and technical settings. It recognizes under-explored issues such as AI risks, cross-cultural privacy standards, and enforcement vacuums, and suggests future directions for multi-disciplinary solutions. The studies considered offer varied but complementary viewpoints: DeVries [1] stresses that privacy rights need to be reinterpreted both legally and ethically in the digital era. Masood [2] brings forth the manner in which concerns for privacy influence political engagement, especially in polarized contexts. Shozi and Mtsweni [3] observe that though social networks facilitate communication, they subject users to great risks of exploitation of data. Bonneau and Preibusch [4] refer to the digital world as a "privacy jungle" wherein users are not in control and informed. Di Minin et al. [5,15] discuss the use of social media data ethically in conservation science, emphasizing adherence to guidelines such as GDPR. Ahmad [6] discusses the misuse of information voluntarily provided, mirroring both user accountability and loopholes for regulation. Alrayes and Abdelmoty [7] expose mismatch between user expectations and current privacy behaviors within the MENA region. Gruzd and Hernández-García [8] research changing digital

* Corresponding author: Manikantan R

norms and how they influence willingness to share sensitive information. Zhang and Shen [9] analyze privacy threats in big datasets. Yadav and Tiwari [10] emphasize the importance of privacy-preservation tools in low-resource environments. Thompson [11] discusses ethical paradoxes in implementing Western views of privacy worldwide. Kumar [12] mathematically models data leakage, providing analytical tools for threat estimation. Reddy et al. [13] attribute social media growth to deepening breaches and surveillance. Boyd and Ellison [14] attribute initial privacy issues to social media design architecture. Sarikakis and Winter [16] indicate that most individuals do not know their rights in the law with regards to data. Facebook Inc. [17] positions surveillance capitalism as an emerging economic paradigm for digital platforms. Smith [18] illustrates privacy as a moving target from the dynamics of fast technological evolution. Gupta and Sharma [19] record threats such as phishing and profiling. Wenzel and Kumar [20] point out users' perceptions of platform safety and the reality between them.

2. Methodology

We conducted a narrative review, gathering twenty peer-reviewed articles selected for their applicability to social media privacy. The research covers the 2003–2024 period and employs various geographical locations and methodological strategies. For a thorough review, we browsed IEEE Xplore, SpringerLink, ACM Digital Library, and Scopus, employing keywords like "data privacy," "social media," "user awareness," "GDPR," "privacy-preserving technologies," and "data protection frameworks." The chosen studies were classified into four broad categories: User Awareness, Legal Frameworks, Risks and Threats, and Privacy-Preserving Technologies. Classifying the literature in a thematic manner aided us in understanding more clearly the interplays between user behaviour, policy, and innovation.

- DeVries [1] applied legal analysis to discern constitutional principles with reference to digital privacy.
- Masood [2] utilized a cross-cultural comparative survey to examine user attitudes and behaviour.
- Shozi and Mtsweni [3] applied qualitative analysis and case studies to investigate data privacy in African social media environments. Bonneau and Preibusch [4] conducted economic and usability analysis of 45 platforms in order to gain insights into privacy market dynamics.
- Di Minin et al. [5,15] applied ethical risk frameworks and policy compliance assessment against GDPR for the use of conservation science data.
- Ahmad [6] applied theoretical framing and user behaviour analysis in legal scenarios.
- Alrayes and Abdelmoty [7] applied quantitative survey research in MENA countries using statistical modeling. Gruzd and Hernández-García [8] examined patterns of disclosure with thematic content analysis. Zhang and Shen [9] utilized graph-based anonymization models and simulation with algorithms. Yadav and Tiwari [10] experimented with cryptographic techniques with prototype software for the Android platform. Thompson [11] employed ethical argumentation and philosophical analysis in cross-border privacy law. Kumar [12] built mathematical models to simulate data exposure threats. Reddy et al. [13] employed a systematized review combining technology and ethical lenses.
- Boyd and Ellison [14] executed historical and sociological case studies.
- Sarikakis and Winter [16] canvassed users' legal awareness through mixed-methods instruments.
- Facebook Inc. [17] carried out longitudinal and economic systems reviews.
- Smith [18] employed legal literature analysis and conceptual frameworks. Gupta and Sharma [19] synthesized a large body of literature and attack vector taxonomy.
- Wenzel and Kumar [20] employed survey measures and regression analysis to relate trust and data-sharing behaviour.

Such diverse methods lead to a more nuanced, multi-faceted understanding of social media site privacy.

3. Literature review

This section provides an overview of existing work on data privacy in social media, categorized into four broad sections: User Behaviour and Awareness, Legal Frameworks and Privacy Policies, Risk and Threats to Privacy, and Privacy-Saving Technologies. Each topic is abstracted, evaluated, and related to gaps in the literature.

- User Awareness and Behaviour: Users are at the same time both the owners of data privacy and the weakest point in its protection. Alrayes and Abdelmoty [7] discovered that, although users are concerned with privacy, their behavior rarely aligns with these concerns. Their MENA survey indicated significant differences between city and rural dwellers, and awareness is strongly correlated with education level. Gruzd and Hernández-García [8] emphasized context collapse in which fuzzy boundaries between private and public sharing result in inadvertent oversharing. Boyd and Ellison [14] demonstrated how early social media designs fostered visibility,

a practice that continues. Ahmad [6] indicated that even long-time users misconceive default privacy settings and seldom review them. Thompson [11] contended that cultural variance renders one privacy design standard unsuitable for all situations.

- Critique: Studies stress user responsibility but usually overlook how platform design itself influences risky practices. There are few studies suggesting definitive literacy interventions.
- Gap: Limited investigation of user awareness in low-literacy and non-Western populations.

- Privacy Policies and Regulating Frameworks: Regulating frameworks like the GDPR, CCPA, and national data protection legislations help ensure the protection of users, with the studies reviewed showing mixed success with enforcement and sensitization. DeVries [1] laid out core tensions between free speech and privacy, showing that legal frameworks have to constantly develop. Sarikakis and Winter [16] coined the term 'legal consciousness' and demonstrated through qualitative interviews that users tend to be aware they have rights but are unclear on what these rights are or how to do something about them. Wenzel and Kumar [20] supplemented quantitative information, indicating that a majority of users consider platforms to be GDPR-compliant, even when the evidence indicates they are not. Di Minin et al. [5,15] highlighted the fact that researchers handling social media data have to walk carefully, even if data is publicly available, given that user assumptions tend to presume privacy. Kumar [12] took it one step further by employing mathematical modelling to illustrate regulatory protections being lacking when data traverses jurisdictions Smith [18] discussed how legal tools tend to trail technological progress, and the need for more responsive, principle-based data governance. Thompson [11] and Ahmad [6] both concluded that regulatory texts must be made available to non-specialist readers to bridge the gap between legality and usability. Whereas users are struggling to grasp, legislation such as the GDPR and CCPA seeks to bridge the gap by making the platforms accountable. DeVries [1] laid out the underlying tension between government regulation and user freedom. Sarikakis and Winter [16] posited that most users are vaguely conscious of their rights according to such systems. Wenzel and Kumar [20] found a large issue: perception of safety. Most believe popular sites are fully compliant with the law, when enforcement is sporadic and there are numerous loopholes. Thompson [11] took an ethical approach and identified the challenge of enforcing these laws in low-literacy environments or across cultural differences in understanding privacy. Smith [18] and Di Minin et al. [5,15] further emphasized that regulation tends to fall behind innovation. This leaves a legal gray area, especially in scenarios where AI, biometrics, and behavioural profiling are used with limited control. The literature proposes that international cooperation and legal flexibility are necessary to effectively protect user privacy.
  - Critique: Although these studies demonstrate the importance of law, none of them presents useful means to enforce regulations across borders.
  - Gap: No research on the enforcement of developing countries and how to simplify dense legal texts to make them usable by the average person.
- Privacy Risks and Threats: The social media privacy risk environment is dynamic and multi-faceted. Bonneau and Preibusch [4] used the term 'privacy jungle' to characterize the lopsided environment in which user protections are thin and uneven. They charted the different business models of social media sites, observing how monetization strategies for data tend to happen at the cost of well-informed user consent. Shozi and Mtsweni [3] examined the platform technical architecture, pinpointing insecure APIs and third-party app integrations as significant vulnerabilities. Gupta and Sharma [19] discovered that platform design decisions—like not enabling two-factor authentication by default or imprecise consent paths—are frequently used to amplify phishing attacks. Masood [2] had a more political sociological perspective in describing how surveillance (both corporate and state) influences user politics and political engagement. Facebook Inc. [17] gave a critical review of their own data harvesting practices, providing insight into the ways that surveillance capitalism monetizes every click and scroll of every user. Smith [18] and Boyd and Ellison [14] argued that user profiling and algorithmic bias create new ethical dangers beyond data breaches and leaks. Most of the papers considered here consider privacy threats as a growing, dynamic threat. Bonneau and Preibusch [4] referred to today's online world as a "privacy jungle," in which visitors have to navigate alone in a foggy maze of terms, tracking codes, and information brokers. Masood [2] found that actually, fear of surveillance deters civic engagement on the web, particularly among politically active users. Shozi and Mtsweni [3] explained how third-party apps introduce vulnerabilities, usually without actually knowing how deep their access is. Gupta and Sharma [19] also showed again how phishing and social engineering attacks take advantage of platform vulnerabilities. Even innocuous attributes like personal suggestions or facial recognition can go up in smoke if not used responsibly. Such examples attest to the fact that privacy is not a technical problem at all—it's psychological and emotional too. Users have the right to trust their systems, not just tolerate them.
  - Critique: Research reveals threats but tends to fall short of quantifying their actual social impact on user trust and civic discourse.
  - Gap: Requirement for cross-cultural comparisons of risk perception and risk management.

- 4) Privacy-Preserving Technologies : The technological edge of privacy is constantly advancing, but the literature indicates a disconnect between innovation and uptake. Yadav and Tiwari [10] suggested attribute-based encryption tailored for mobile devices with low computation overhead for users in low-bandwidth areas. Zhang and Shen [9] came up with scalable graph anonymization methods that guarantee differential privacy for big data. Reddy et al. [13] recommended hybrid architectures that integrate federated learning, blockchain, and edge computing to decentralize control and reduce data exposure. Kumar [12] used mathematical logic to model the likelihood of re-identification in joint datasets and provided actionable thresholds for anonymization. Thompson [11] and Ahmad [6] also brought up an important point—users tend to distrust sophisticated technologies that they cannot comprehend. This observation indicates that effective privacy products should be explainable as well as embedded naturally in platform user interfaces. Di Minin et al. [5] and Gruzd and Hernández-Garca [8] reinforced this by calling for participatory design in the design of privacy technologies to guarantee user-centric functionalities. Despite these developments, few solutions have gained traction. The reasons are economic and technical: lack of standardization, platform resistance to engagement metrics, and low user awareness. The articles before us agree—technology alone cannot solve privacy unless in a supportive legal and cultural environment. Confronted with these threats, innovation is not halted. Yadav and Tiwari [10] presented lightweight encryption algorithms that make data protection affordable even for less expensive phones. Zhang and Shen [9] examined anonymization techniques that preserve user identity without compromising data utility. Differential privacy frameworks were introduced by Kumar [12] that mathematically protect user identity. Real-world adoption is limited, however. As noted by Reddy et al. [13], platforms have few business reasons to deploy such solutions. Some research proposes mixing new technologies—such as federated learning, blockchain, and AI—to develop the next generation of privacy solutions. Hybrid models are promising but require defining clear standards and improved user communication to achieve mainstream success.
  - Critique: Research provides technical novelty with minimal insight into usability and mass deployment.
  - Gap: Inadequate practical application and absence of standards for new technologies such as federated learning and decentralized identities.

Author	Year	Focus	Key Findings	Limitations
Alrayes & Abdel Moty	2024	User Awareness (MENA)	Awareness shaped by education, demographics	Region-specific, not global
DeVries	2003	Legal Principles	Free speech vs. privacy rights	Outdated in AI era
Bonneau & Preibusch	2010	Risks/Business Models	"Privacy jungle," weak protections	Limited to early platforms
Yadav & Tiwari	2023	Encryption	Lightweight, mobile-friendly	Low adoption, usability challenges
Reddy et al.	2016	Hybrid Architectures	Blockchain + federated learning	Lacks real-world testing
Wenzel & Kumar	2020	Trust & Legal Compliance	Users overestimate GDPR compliance	Survey bias, no cross-country data

Figure 1 Comparative Summary Table

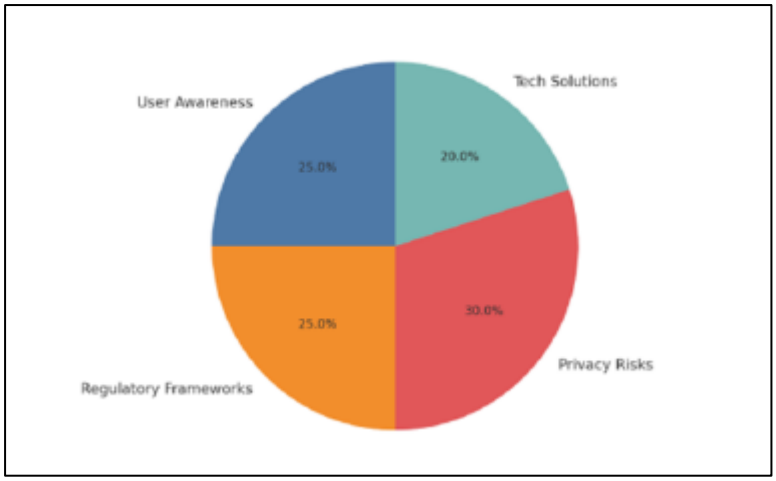

Figure 2 Distribution of Reviewed Papers by Privacy Theme

3.1. Analysis of Gen-Z Social Media Behaviour in India

Young Indians often use social media for social bonding and self-expression. They engage in minimal interaction with terms of service or privacy settings. They tend to publicly share by default, boosting risks of exposure to misinformation, impersonation, and unwanted surveillance [4], [7], [8]. Behavioral aspects, including peer approval and cultural collectivistic focus, impact the decisions made in sharing data. These findings highlight the need for localized perspective in designing privacy solutions.

3.2. Privacy Threats and Models

Threats of social media usage are multidimensional:

- Internal:: Monitoring by platforms, data excess, uncontrolled analytics [12], [14].
- External:: Social engineering, identity theft, scraping bots [10], [11].
- User-sourced:: Lack of understanding privacy settings, compulsive posting, and peer pressure [1], [8].Systematic categorizations of these threats have been presented in threat models by Shozi and Mtsweni and Kayes and Iamnitchi, in support of comprehensive defense strategies.

Legal and Regulatory Overview: Regulations governing data privacy are

- GDPR – Robust protections with minimal global application.:
- DPDP (India) – A fresh 2023 act emphasizing localization of data and informed consent :
- CCPA – An American law that provides rights over personal data.:

Technical Safeguards and Frameworks: New technologies provide several solutions:- Anonymization methods: Useful but can lower data usefulness. Federated learning: Leaves data on-device, encouraging privacy [12].- Decentralized identities: Facilitate user control but are computationally costly. - Access control models: Apply selective sharing on the basis of user-specified roles [14]. While models like that of Yadav and Tiwari use both encryption and steganography for improved security, they tend to lack accessibility features to facilitate large-scale adoption.

4. Discussion

The evidence considered here clearly lays down that social media data privacy is a system-level, multidimensional, and speeding issue and not a sector- or stakeholder-bounded issue Research Saturation vs. Underexplored Areas The literature is strong on user awareness, platform regulatory issues, and platform structural problems in Western contexts. Alrayes and Abdelmoty [7] and Gruzd and Hernández-García [8] consistently demonstrate that privacy issues are raised by users but are not generally followed up with informed action or knowledge of site policies. Privacy on non-Western social media sites, ethical issues beyond legality, and privacy in new digital services are under-explored.

Unresolved Problems: Regulation is necessary but not enough. According to DeVries [1], Sarikakis and Winter [16], and Wenzel and Kumar [20], even strong legal tools such as GDPR and CCPA are watered down by loopholes in enforcement

and low user awareness levels. Moreover, monetization and surveillance designs of websites, weighed down by Bonneau and Preibusch [4] and Masood [2], construct structural impediments to self-regulation, and so intrinsic incentives become inevitable. Technologies like attribute-based encryption [10], differential privacy [12], and federated learning [13] are promising but currently suffer from a lack of usability. They will only work if end users are able to comprehend and believe them, whereupon Thompson [11] and Ahmad [6] build foundations. Shifting Privacy Concerns and Emerging Issues. While focus here is not so much on AI, new technologies continue to pose new vectors for privacy. Aggregation of data by automated means, algorithmic profiling, and data-driven personalization make transparency and consent difficult. These trends worsen existing gaps in user understanding and regulation that render privacy a moving target Policy Gaps There are laws in various jurisdictions but fragmented global enforcement. Misalignments between claims by platforms of compliance and effective protective steps demonstrate enforcement shortcomings. Cross-border data flows, differing interpretations of regulations, and non-coordinated authorities put users at risk despite so-called protectio. Future Directions All these challenges call for multidisciplinary collaboration. Legal scholars, technologists, designers, and users need to collaborate in addressing the creation of systems that are adaptive, resilient, and context-sensitive. Scholarship needs to be aimed at unexamined contexts such as privacy practice in non-Western social media, ethical models other than legalistic compliance, and user-centric approaches towards the adoption of privacy-protective technologies. Briefly, social media privacy is a persistent and recurring issue that needs to be treated using technology astuteness and comprehensive, contextual approaches to regulation, education, and platform accountability.

5. Conclusion

Social media data privacy is an ongoing negotiation, not a solvable problem. Users, platforms, and governments must all do their share. The 20 papers we discussed here offered diverse views but share one message: we must have systems that are not just private by design, but private by default, and human-centred in nature. This review shows that while technical solutions and regulatory frameworks are changing, they still remain disconnected with user behaviour and expectations. Greater transparency in policy, better user interface design, and technology development participation are needed. It is also clear that privacy cannot be ensured via technology or legislation alone—it requires literacy in society and cultural change. The books call for a shift away from reactive to proactive approaches to data protection. These include anticipatory regulation, ethical-by-design, and live user education. As social media continues to evolve with AI, biometrics, and immersive platforms, the future of privacy will demand interdisciplinary effort and continued watchfulness. New research scholars have to turn to marginalized groups, cross-cultural ethics, and concrete policy impacts. In short, data privacy has to be thought of as a fundamental digital right. Achieving this takes more than technology or statute—it takes lasting commitment, open conversation, and trust-based systems, that respect the dignity of all users in a networked world.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] W. T. DeVries, “Protecting privacy in the digital age,” *Berkeley Tech. LJ*, vol. 18, p. 283, 2003.

[2] S. Ahmed and M. Masood, “Assessing the effects of privacy concerns on social media-driven political discussions and participation: A comparative study of asian and western contexts,” *Social Science Computer Review*,vol.43, no. 1, pp.67–88,2025.

[3] N. A. Shozi and J. Mtsweni, “Big data privacy in social media sites,” in *2017 IST-Africa Week Conference (IST-Africa)*. IEEE, 2017, pp.1–6.

[4] J. Bonneau and S. Preibusch, “The privacy jungle: On the market for data protection in social networks,” in *Economics of information security and privacy*. Springer, 2010, pp. 121–167.

[5] E. Di Minin, C. Fink, A. Hausmann, J. Kremer, and R. Kulkarni, “How to address data privacy concerns when using social media data in conservation science,” *Conservation Biology*, vol. 35, no. 2, pp. 437–446, 2021.

[6] N. Ahmad, “Data privacy issues and risks with sharing on social media: An inquiry,” *Russian Law Journal*, vol.11,no.4,pp.597–611,2023.

[7] A. Farooq, J. Salminen, J. D. Martin, K. Aldous, S.-G. Jung, and B. J. Jansen, "Exploring social media privacy concerns: A comprehensive survey study across 16 middle eastern and north african countries," *IEEE Access*,vol.12,pp.147087–147105,2024.

[8] A. Gruzd and Á. Hernández-García, "Privacy concerns and self-disclosure in private and public uses of social media," *Cyberpsychology, Behavior, and Social Networking*, vol. 21, no. 7, pp. 418–428, 2018.

[9] Y. Gao, Y. Li, Y. Sun, Z. Cai, L. Ma, M. Pustisek, and S. Hu, "Ieee access special section: privacy preservation for large-scale user data in social networks," *IEEE access*, vol. 10, pp. 4374–4379, 2022.

[10] S. Yadav and N. Tiwari, "Privacy preserving data sharing method for social media platforms," *PloS one*, vol.18, no. 1,p.e0280182,2023.

[11] L. Nemec Zlatolas, L. Hrgarek, T. Welzer, and M. Höbl, "Models of privacy and disclosure on social networking sites: a systematic literature review," *Mathematics*, vol.10, no. 1, p. 146, 2022.

[12] K. Saravanakumar, K. Deepa *et al.*, "On privacy and security in social media–a comprehensive study," *Procediacomputerscience*, vol.78,pp.114–119, 2016.

[13] A. Ho, A. Maiga, and E. Aimeur, "Privacy protection issues in social networking sites," in *2009 IEEE/ACS International Conference on Computer Systems and Applications*. IEEE, 2009, pp. 271–278.

[14] K. Sarikakis and L. Winter, "Social media users' legal consciousness about privacy," *Social Media+ Society*,vol.3,no.1,p.2056305117695325,2017.

[15] L. Edwards, "Privacy, law, code and social networking sites," in *Research handbook on governance of the internet*. Edward Elgar Publishing, 2013, pp.309–352.

[16] S. Rewaria, "Data privacy in social media platform: Issues and challenges," *Available at SSRN 3793386*, 2021.

[17] D. L. Gazzoni Filho and P. S. L. M. Barreto, "Demonstrating data possession and uncheatable data transfer, "*cryptologye Print Archive*,2006.

[18] I. Kayes and A. Iamnitchi, "Privacy and security in online social networks: A survey," *Online Social Networks and Media*, vol. 3, pp. 1–21, 2017.