e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:04/April-2025 Impact Factor- 8.187 www.irjmets.com

PERCEIVED RISKS OF DATA SHARING ON SOCIAL MEDIA

Prof. Amita Garg*1, Balas Kinjal*2, Umang Srivastav*3

*1,2,3Parul University, India.

DOI: https://www.doi.org/10.56726/IRJMETS71949

ABSTRACT

The rapid proliferation of social media platforms has revolutionized how people communicate, share information, and engage in online communities. However, the convenience of online interaction comes with significant risks, including privacy breaches, identity theft, cyberstalking, and unauthorized data exploitation. This study explores the perceived risks of data sharing on social media by analyzing user concerns, behavioral patterns, and security awareness. Using a mixed-methods research approach, which includes surveys and interviews, we evaluate factors influencing risk perception and investigate potential mitigation strategies. The findings highlight the importance of digital literacy, regulatory frameworks, and advanced security measures in enhancing user safety. The study provides actionable recommendations to improve user awareness and promote safer social media practices.

Keywords: Data Privacy, Cybersecurity, Social Media Risks, Identity Theft, Privacy Awareness, Digital Literacy.

I. INTRODUCTION

Social media platforms have significantly transformed global communication, allowing users to share personal, professional, and social information instantly. While this has enhanced connectivity, it has also introduced substantial privacy and security risks. Cybercriminals exploit user data for malicious purposes, including identity theft, targeted phishing attacks, cyberstalking, and financial fraud. Despite efforts by social media companies to implement security measures, many users remain unaware of these threats or fail to adopt effective preventive measures.

This study investigates how users perceive the risks associated with data sharing on social media. By examining privacy concerns, behavioral tendencies, and security awareness, we aim to provide insights into how users can safeguard their information while maintaining an active online presence.

II. LITERATURE REVIEW

Alrayes et al. (2020) explored the perceived risks of disclosing location data on social networking sites. The study utilized a sample of 715 participants and applied modeling techniques to identify the underlying factors influencing privacy concerns. Results showed that users' perceptions of privacy risk are heightened when location data is shared publicly or without control mechanisms. The findings stress the need for context-aware privacy settings and transparency in data use to mitigate user concerns.

Van Schaik et al. (2018) examined users' security and privacy risk perceptions on Facebook and their corresponding precautionary behaviors. Through quantitative methods, the study found that users who perceive higher risks are more likely to take protective actions such as adjusting privacy settings or limiting content shared. The study emphasized that perceived privacy risks serve as strong predictors of defensive digital behavior.

Koohang, Paliszkiewicz, and Goluchowski (2018) focused on the relationship between users' trust and risk beliefs in the context of social media. Their findings revealed that privacy concerns negatively impact trusting beliefs and simultaneously elevate perceptions of risk. This indicates that the more users fear privacy breaches, the less trust they place in the platform, which in turn affects their willingness to engage or share data. **Dhir et al. (2017)** investigated the link between online privacy concerns and selfie behavior across various age groups. The study found that adolescents and young adults with stronger privacy concerns were less likely to share selfies online. This negative relationship highlights how privacy concerns can significantly shape users' self-presentation behaviors on social media.

Kokolakis (2017) conducted a comprehensive review of the "privacy paradox"—a phenomenon where users express concern about privacy but still disclose personal information online. The review identified

psychological, contextual, and design factors that contribute to this inconsistency. The paper argues that addressing this paradox requires better interface design and user education.

Taddicken (2014) studied the impact of privacy concerns and social relevance on self-disclosure behaviors in social media. Her findings suggested that even individuals with high privacy concerns still engage in self-disclosure when they perceive the social rewards to be high. This supports the idea that personal and social motivations often override risk awareness.

Debatin et al. (2009) analyzed Facebook users' privacy attitudes, behaviors, and the unintended consequences of their online actions. The study found a disconnect between users' awareness of privacy issues and their actual online behavior, suggesting limited effectiveness of current privacy education or tools.

Krasnova et al. (2010) explored the reasons users share personal information despite known privacy risks. The study concluded that intrinsic motivations—such as the desire for social connection—often outweigh privacy concerns. This highlights the complexity of users' privacy calculus when engaging in digital communication.

Marwick and Boyd (2014) focused on how teenagers manage privacy through context negotiation on social media. Their findings revealed that teens actively tailor their online content to suit different audiences, demonstrating a nuanced understanding of privacy, even if traditional privacy tools are underutilized. **Khoa and Vi (2021)** studied the negative impact of perceived privacy risks on consumer information sharing on Facebook. The research emphasized that users who fear privacy breaches are significantly less willing to share personal data, highlighting the importance of perceived safety in encouraging engagement. **Gerhart and Koohikamali (2020)** applied the privacy calculus model to understand how users weigh privacy concerns against perceived benefits when using social media apps. Their study found that users are willing to engage if they perceive high utility, even when privacy concerns exist—emphasizing the trade-off mindset in digital decision-making.

Ozdemir, Smith, and Benamati (2017) examined the antecedents of privacy concerns in peer-based social media interactions. Their results indicated that peer influence, past experiences, and platform design are key drivers of privacy concern, which in turn impacts how users control their information-sharing behavior. **Trepte and Masur (2017)** conducted a cross-cultural study comparing German and U.S. users' attitudes towards privacy and self-disclosure. Findings showed that cultural values significantly affect privacy expectations and behaviors, with German users displaying more caution compared to their American counterparts.

Bol, Dienlin, and Ström (2018) extended the privacy calculus theory by incorporating cultural and boundary regulation aspects. The study demonstrated that users employ various boundary-management strategies based on cultural norms, influencing how much they disclose and to whom.

Baruh, Secinti, and Cemalcilar (2017) provided a meta-analysis on online privacy concerns and management strategies. They synthesized findings from multiple studies to identify patterns in how users manage privacy risks, noting that individual differences and contextual factors heavily mediate privacy-related decisions. **Masur and Scharkow (2016)** examined how risk perception and privacy concerns shape disclosure strategies. Their research supported the privacy paradox, showing that even concerned users often disclose personal information due to habit, social pressure, or perceived benefits.

Chang, Liu, and Shen (2017) compared user trust between Facebook and LinkedIn. The study revealed that users' trust was shaped by platform-specific factors, with LinkedIn perceived as more professional and secure, leading to different information-sharing behaviors than on Facebook.

Vitak and Kim (2014) investigated how Facebook's technical features influence user disclosure and interpersonal boundary management. They found that while tools like blocking and custom audience selection are helpful, they don't fully account for the complexities of real-life relationships and disclosure dilemmas.

Research Objectives:

1. To assess user awareness regarding the risks of data sharing on social media.
2. To analyze the impact of demographic and personal factors on risk perception.
3. To examine the effectiveness of privacy settings and cybersecurity measures.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:04/April-2025 Impact Factor- 8.187 www.irjmets.com

4. To propose strategies for improving data security and user awareness

III. RESEARCH METHODOLOGY

Data Collection

A mixed-methods research approach, incorporating surveys and structured interviews, was used to collect data from social media users across different demographics.

Sampling Technique

Stratified random sampling was used to ensure diverse representation across age groups and user demographics.

Survey Categories

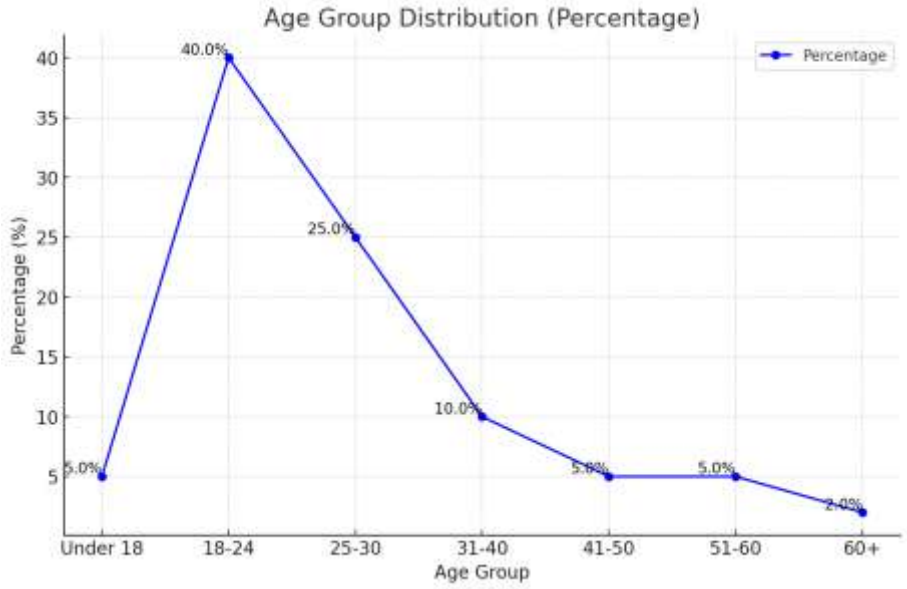
1. Awareness of privacy risks
2. Frequency and type of data shared online
3. Experiences with privacy breaches or cyber threats
4. Use of privacy settings and security tools

Data Analysis

Descriptive statistical analysis was used to identify trends, and a chi-square test was employed to determine the statistical significance of variations in user behavior across demographic groups.

IV. RESULTS AND DISCUSSION

The findings indicate that data-sharing behaviors on social media vary significantly across age groups. Users aged 18-24 exhibit the highest level of data sharing, while older users demonstrate more caution. Privacy settings review frequency shows that only 16.2% of users consistently review their settings, whereas 37.1% do so occasionally. The low adoption of security measures highlights the need for improved digital literacy and awareness campaigns. The results suggest a strong correlation between age, awareness, and privacy practices. To enhance security, social media platforms must implement clearer privacy policies, automated alerts, and user-friendly security tools.



Analysis of Age Group Distribution in Social Media Engagement

The age group distribution in social media engagement reveals important trends about digital behaviour across different demographics. Understanding these patterns helps businesses, marketers, and policymakers tailor their strategies to effectively reach specific age groups.

From the data, the 18-24 age group shows the highest engagement, contributing 40% of total social media participation. This demographic is highly active online, using social media for communication, entertainment, and information. Their strong presence makes them the primary audience for digital marketing, influencer

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:04/April-2025 Impact Factor- 8.187 www.irjmets.com

collaborations, and viral content. Platforms like Instagram, TikTok, and Snapchat dominate this segment, offering visually-driven and interactive experiences that appeal to younger users.

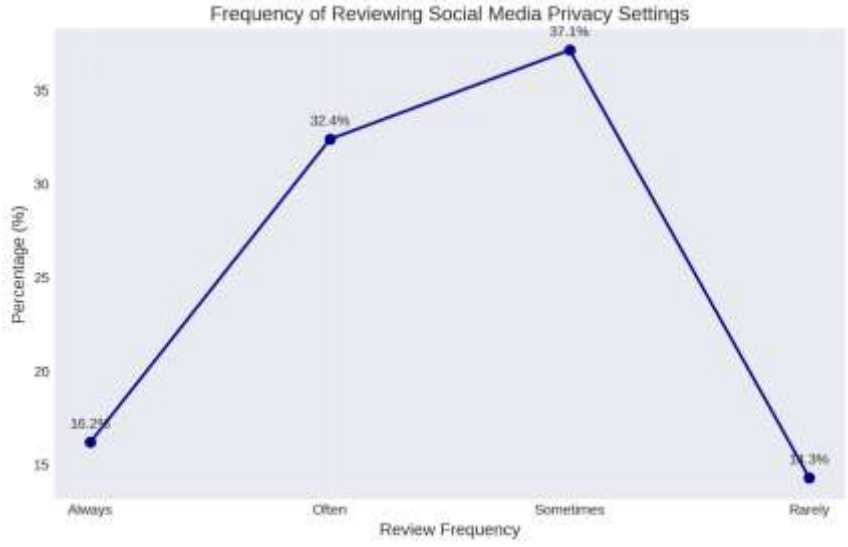
The 25-30 age group follows closely, accounting for 25% of engagement. While slightly lower than the younger group, this demographic remains highly active online. Many individuals in this age range are early professionals or entrepreneurs who utilize social media for business networking, career opportunities, and industry updates. LinkedIn, Twitter, and Facebook serve as popular platforms for this group, reflecting their professional and informational needs.

Engagement declines significantly in the 31-40 age group, which comprises 10% of total participation. At this stage, social media consumption becomes more selective, with users focusing on career-related content and personal development. Many in this demographic have increased professional and family responsibilities, reducing their discretionary screen time. While they continue to engage with social media, their participation is often limited to informative and practical content rather than casual browsing.

The 41-50 and 51-60 age groups each contribute only 5% of total engagement. Middle-aged individuals often prefer traditional communication methods and may be less inclined toward social media interaction. Privacy concerns, unfamiliarity with new digital trends, and a preference for real-world interactions contribute to their lower participation. However, social media platforms that emphasize trust, accessibility, and informational content could potentially increase their engagement.

The 60+ age group has the lowest engagement level at just 2%. Many older individuals still rely on traditional media for news and communication, and they may find social media complex or unappealing. However, digital literacy programs and user-friendly interfaces designed for seniors could help boost their participation in the future.

Overall, the data highlights that younger users dominate social media, while older demographics engage less frequently. Businesses should focus on visually engaging, interactive content for younger audiences while providing informative, trustworthy content for older users. Understanding these trends enables companies to design targeted marketing strategies, ensuring inclusivity across all age groups.



The chart titled "Frequency of Reviewing Social Media Privacy Settings" presents data on how often individuals check their privacy settings on social media platforms. The x-axis represents four frequency categories—Always, Often, Sometimes, and Rarely—while the y-axis displays the percentage of respondents for each category.

From the chart, 16.2% of respondents fall under the "Always" category, indicating that a portion of users consistently monitor and adjust their privacy settings. These individuals are highly aware of online security risks and actively take measures to protect their personal information. The "Often" category comprises 32.4% of respondents, representing users who review their privacy settings regularly but not as frequently as the first group. This suggests a strong awareness of digital security, though some users may check their settings only

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:04/April-2025 Impact Factor- 8.187 www.irjmets.com

when prompted by platform updates or security concerns. The largest portion, 37.1% of respondents, falls into the "Sometimes" category. This indicates that a significant number of individuals occasionally check their privacy settings but do not do so regularly. These users may be aware of privacy risks but may not prioritize reviewing their settings unless they encounter a specific concern, such as an unexpected data breach or unauthorized access to their account. The "Rarely" category accounts for 14.3% of respondents, representing those who seldom check or adjust their privacy settings. These individuals are at a higher risk of privacy breaches, as they may be unaware of security vulnerabilities or changes in social media policies. Their lack of engagement may stem from unfamiliarity with privacy settings, lack of concern about data security, or the assumption that their default settings provide adequate protection.

The overall distribution of responses highlights a mixed approach to privacy management among social media users. While a significant percentage actively engage in reviewing their settings, a considerable portion remains passive. This suggests a need for increased digital literacy, awareness campaigns, and simplified privacy control options to encourage better security habits.

By leveraging these insights, social media platforms and cybersecurity professionals can implement strategies to enhance user engagement with privacy settings. Notifications, user-friendly privacy dashboards, and educational initiatives can help ensure that more individuals take proactive steps to protect their online information.

V. CONCLUSION

The perceived risks of data sharing on social media continue to be a critical concern in the digital age. As highlighted in the literature, privacy concerns, identity theft, cyberstalking, and data exploitation pose significant threats to users. Despite awareness of these risks, many users engage in unsafe data-sharing behaviors due to convenience, lack of understanding, or trust in social media platforms. The increasing volume of personal information shared online has made users more vulnerable to cyber threats, emphasizing the need for stricter privacy controls and user education.

To mitigate these risks, social media platforms must implement more robust security measures, such as end-to-end encryption, AI-driven threat detection, and multi-factor authentication. Additionally, user-friendly privacy policies should be introduced to enhance transparency and ensure users are well-informed about how their data is collected, stored, and used. Educational initiatives that promote digital literacy and privacy-conscious behavior can further empower users to make safer decisions when sharing personal information.

VI. FUTURE SCOPE

The future scope of this research lies in exploring advanced cybersecurity measures that can further protect users from data breaches and unauthorized access. The integration of blockchain technology for secure data transactions, the use of machine learning algorithms for real-time threat detection, and the development of personalized privacy settings based on user behavior are potential areas for future investigation.

As technology evolves, ongoing research and policy development will be essential in addressing emerging threats, ensuring that social media remains a secure and trustworthy environment for all users.

Step 1: Hypotheses

- **Null Hypothesis (H_0):** Age group and frequency of reviewing privacy settings are independent.
- **Alternative Hypothesis (H_1):** Age group and frequency of reviewing privacy settings are dependent.

Step 2: Observed Data (O)

Age Group	Always	Often	Sometimes	Rarely	Never	Total
Under 18	1	1	2	1	0	5
18–24	6	10	16	9	1	42
25–30	4	6	10	6	0	26
31–40	2	4	6	4	0	16

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:04/April-2025 Impact Factor- 8.187 www.irjmets.com

Age Group	Always	Often	Sometimes	Rarely	Never	Total
41–50	1	2	3	2	0	8
51–60	1	1	2	1	0	5
60+	0	1	1	0	0	2
Total	**15**	**24**	**40**	**23**	**1**	**105**

Step 3: Expected Frequencies (E)

Calculated as **(Row Total × Column Total) / Grand Total**

Example for Under 18 - Always:

E = (5 × 15) / 105 = **0.71**

Expected frequencies are similarly computed for all cells.

Step 4: Chi-Square Formula

$\chi^2 = \sum(O-E)^2 / E$

Sample:

(Observed: 1, Expected: 0.71) → $(1-0.71)^2 / 0.71$ = **0.118**

Sum of all contributions:

Age Group	χ^2 Contribution
Under 18	0.2344
18–24	1.1097
25–30	0.3568
31–40	1.6122
41–50	0.7689
51–60	0.2210
60+	1.6265
Total	**5.9295**

Step 5: Degrees of Freedom

df = (Rows−1)(Columns−1) = (7−1)(5−1) = **24**

Step 6: Critical Value

At α = 0.05, df = 24 → Critical χ^2 = **36.415**

Step 7: Conclusion

Since $\chi^2 = 5.9295 < 36.415$, we **fail to reject H_0**.

Final Conclusion

There is **no significant relationship** between age group and the frequency of reviewing privacy settings on social media. Different age groups behave similarly in this context.

VII. REFERENCES

[1] Alrayes, F. S., Abdelmoty, A. I., El-Geresy, W. B., & Theodorakopoulos, G. (2020). Modelling perceived risks to personal privacy from location disclosure on online social networks. International Journal of Geographical Information Science, 34(1), 150–176. https://doi.org/10.1080/13658816.2019.1654109

[2] van Schaik, P., Jansen, J., Onibokun, J., Camp, J., & Kusev, P. (2018). Security and privacy in online social networking: Risk perceptions and precautionary behaviour. Computers in Human Behavior, 78, 283–297. https://doi.org/10.1016/j.chb.2017.10.007

[3] Koohang, A., Paliszkiewicz, J., & Goluchowski, J. (2018). Social media privacy concerns: Trusting beliefs and risk beliefs. Industrial Management & Data Systems, 118(6), 1209–1228.

https://doi.org/10.1108/IMDS-12-2017-0558

[4] Dhir, A., Torsheim, T., Pallesen, S., & Andreassen, C. S. (2017). Do online privacy concerns predict selfie behavior among adolescents, young adults and adults? Frontiers in Psychology, 8, 815. https://doi.org/10.3389/fpsyg.2017.00815

[5] Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & Security, 64, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

[6] 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. https://doi.org/10.1111/jcc4.12052

[7] 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. https://doi.org/10.1111/j.1083-6101.2009.01494.x

[8] Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. Journal of Information Technology, 25(2), 109–125. https://doi.org/10.1057/jit.2010.6

[9] Marwick, A. E., & Boyd, D. (2014). Networked privacy: How teenagers negotiate context in social media. New Media & Society, 16(7), 1051–1067. https://doi.org/10.1177/1461444814543995

[10] Khoa, B. T., & Vi, N. D. T. (2021). Consumer information sharing in Facebook: The negative role of perceived privacy risk. Advances in Cyber Security, Communications in Computer and Information Science, 1487, 447–458. https://doi.org/10.1007/978-981-16-8059-5_34

[11] Gerhart, N., & Koohikamali, M. (2020). Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective. Computers in Human Behavior, 107, 106260. https://doi.org/10.1016/j.chb.2020.106260

[12] Ozdemir, Z. D., Smith, H. J., & Benamati, J. H. (2017). Antecedents and outcomes of information privacy concerns in a peer context: The case of social media. International Journal of Information Management, 37(6), 493–502. https://doi.org/10.1016/j.ijinfomgt.2017.05.002

[13] Trepte, S., & Masur, P. K. (2017). Cultural differences in social media use, privacy, and self-disclosure: A comparative study of German and U.S. social media users. New Media & Society, 19(5), 825–849. https://doi.org/10.1177/1461444817705910

[14] Bol, N., Dienlin, T., & Ström, F. (2018). Self-disclosure and privacy calculus on social media: The role of culture and boundary regulation. Frontiers in Psychology, 9, 1908. https://doi.org/10.3389/fpsyg.2018.01908

[15] Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. Journal of Communication, 67(1), 26–53. https://doi.org/10.1111/jcom.12276

[16] Masur, P. K., & Scharkow, M. (2016). Disclosure management on social media: Risk perception, privacy concerns, and the privacy paradox. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 10(1), Article 3. https://doi.org/10.5817/CP2016-1-3

[17] Chang, C.-W., Liu, H.-Y., & Shen, J.-L. (2017). User trust in social networking services: A comparison of Facebook and LinkedIn. Computers in Human Behavior, 69, 207–217. https://doi.org/10.1016/j.chb.2016.12.013

[18] Vitak, J., & Kim, J. (2014). 'You can't block people offline': Examining how Facebook's affordances shape the disclosure process. In Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing (pp. 461–474). https://doi.org/10.1145/2531602.2531672