SUSHANT UNIVERSITY ORGANIZED INTERNATIONAL CONFERENCE ON
"ADVANCES IN MULTIDISCIPLINARY RESEARCH AND INNVOATION" ICAMRI-2023
ON 28-29TH OCTOBER 2023
INTERNATIONAL ADVANCE JOURNAL OF ENGINEERING, SCIENCE AND MANAGEMENT (IAJESM)
July-December 2023, Submitted in October 2023, iajesm2014@gmail.com, ISSN -2393-8048
Multidisciplinary Indexed/Peer Reviewed Journal. SJIF Impact Factor 2023 =6.753

Data Fortification in the Social Sphere: An Exploration through Analytical Hierarchy Process

Vinay Kumar Dawar, Assistant Professor, Sri Aurobindo College of Commerce and Management, Ludhiana, Punjab.
Dr. Karun Kant Uppal, Assistant Professor, P.G. Department of Commerce and Management, Kamla Lohtia SD College, Ludhiana, Punjab.

Abstract

In an era dominated by the rapid evolution of technology and the ubiquitous presence of social media platforms, individuals find themselves seamlessly connected to the world and each other. Social media applications, such as Facebook, Twitter, Instagram, and others, have become integral aspects of modern communication, offering users the ability to share experiences, connect with peers, and explore diverse facets of their surroundings. However, this digital interconnectedness has brought forth a growing concern—data privacy. The conveniences and functionalities provided by social media apps come at the cost of users entrusting significant amounts of personal information to these platforms. As users willingly share their thoughts, preferences, and even geolocational data, a complex web of digital footprints is created. This scenario has raised critical questions about the privacy and security of user data in the digital realm. As a result, this paper tries to figure out the facets that impact the users in deciding the application to be used by the individual. This paper adopts the Analytical Hierarchy Process (AHP) for ranking the different factors influencing the concerns of data privacy while using the social media applications. Various factors are considered in the literature review which becomes the basis of the AHP questionnaire. Priorities are decided among those factors with the help of responses from the respondents. The AHP questionnaire has been filled from the different individual users of Punjab, Haryana and Chandigarh region. The result and findings may diverse in the distinctive region. This study provides insights to the Social media app/website developers to focus on the most important factors that impact the decision of users for selecting any social media for data privacy concerns.

Keywords: Social Media, Data Privacy, Analytical Hierarchy Process, Decision making.

INTRODUCTION

An increasing number of social media networking sites, including Facebook, X (earlier famous with Twitter), Instagram, Telegram, and others, are being developed and launched as a result of the quick growth of technology. They give users the ease to share their lives and explore their surroundings, prevent data silos, and enable them to keep in touch with one another. Unquestionably, social media networking makes people feel more at ease, but it also raises several privacy-related concerns. Even while users are aware of the hazards to their online privacy, they still frequently provide personal information in exchange for specialized or preferred services. It demonstrates the paradoxical psychology of people's concern for privacy. The line that once distinguished privacy between public and private areas is becoming increasingly hazy; therefore, we should make every effort to strike a balance between these two goals, reducing the likelihood that privacy will be revealed as a result of our practice of giving up privacy in exchange for improved services and taking steps to safeguard sensitive information as much as we can.

The majority of study being conducted now focuses on people's perceptions of risk and privacy issues when using social media, as well as the precautions that may be taken to avoid privacy disclosure due to various behaviors. Nevertheless, social media privacy is not categorized. A person's importance of privacy varies, and so do the types of privacy disclosure that result from various behaviors. As a result, it's necessary to quantify the types of privacy disclosure brought about by different user actions on social networks as well as the extent of private disclosure (or protection).

This paper studies the behavior of users of social media toward data privacy concerns. This involves the technique of the Analytical Hierarchy Process through which the priorities will be set to decide which element is impacting the users most while using social media applications.

REVIEW OF LITERATURE

Numerous studies have delved into users' perceptions and awareness of data privacy issues on social media. Acquisti and Grossklags (2005) emphasized the role of individual awareness in influencing privacy concerns, highlighting that users who are more informed tend to be more cautious about sharing personal information. The privacy paradox, a phenomenon where individuals express concerns about privacy but engage in behaviors that compromise it, has been extensively discussed. Taddicken (2014) conducted a comprehensive analysis, suggesting that individuals often grapple with the trade-off between the benefits of social media use and the risks to their privacy. Research has focused on the efficacy of privacy settings and control mechanisms provided by social media platforms. Dwyer, Hiltz, and Passerini (2007) conducted a study on Facebook users, revealing that while privacy settings exist, their complexity often results in users adopting default configurations, inadvertently exposing personal information. High-profile security breaches on social media platforms have fueled research on user trust and its vulnerability. Dinev et al. (2013) explored the aftermath of security incidents, emphasizing the lasting impact on user trust and the imperative for platforms to regain user confidence through enhanced security measures. Cultural factors influencing privacy concerns on social media have gained attention. Xu, Dinev, Smith, and Hart (2011) conducted a cross-cultural study, revealing variations in privacy concerns and behaviors, underscoring the importance of considering cultural nuances in the design of privacy safeguards. With an increasing emphasis on quantitative methodologies, the Analytical Hierarchy Process (AHP) has been employed to prioritize factors influencing privacy decision-making. Li et al. (2014) utilized AHP to assess the significance of different privacy factors, providing a structured approach to understanding user preferences in social media settings. The rise of algorithmic decision-making in social media platforms has spurred investigations into the transparency of these systems. Researchers like Diakopoulos (2016) have emphasized the importance of algorithmic transparency to mitigate privacy concerns, calling for increased user awareness and understanding of the algorithms governing content delivery and personalization. Nissenbaum's contextual integrity framework has been employed to analyze privacy concerns in the context of social media. Researchers, such as Wisniewski and Knijnenburg (2017), applied this framework to scrutinize the appropriateness of information flows in social media environments, contributing to a deeper understanding of privacy norms and expectations. Privacy-intrusive design practices, known as dark patterns, have gained attention as contributors to users unknowingly sharing more information than intended. Brignull and O'Brien (2013) explored the prevalence of dark patterns in social media interfaces, emphasizing the need for ethical design practices to empower users in maintaining control over their personal information. The role of user empowerment and education in mitigating privacy concerns has been a subject of exploration. Tsai and Kelley (2015) investigated the effectiveness of privacy education programs, revealing that informed users are more likely to adopt privacy-preserving behaviors, suggesting the potential for proactive measures in addressing data privacy challenges. Legal and regulatory frameworks play a pivotal role in shaping the landscape of social media privacy. Scholars like Bernal (2016) have examined the effectiveness of existing legal mechanisms in safeguarding user privacy rights and proposed avenues for enhancing legal protections in response to the evolving challenges posed by social media. Trust in social media platforms is a key factor influencing user behavior. Nentwig and Wozniak (2020) conducted a study on user trust, emphasizing the critical role of platform accountability in building and maintaining user trust amidst increasing concerns about data breaches and misuse.

This literature review highlights the diverse avenues explored by scholars to unravel the complexities of data privacy concerns in social media applications. From user perceptions and privacy paradoxes to the role of privacy settings and cross-cultural variations, the literature reflects a nuanced understanding of the challenges posed by the intersection of social media and privacy.

OBJECTIVES OF THE STUDY

- To identify the data privacy concerns that influence the users in deciding the social media application.
- To establish the priority in data privacy concerns that influence the users in deciding the social media application.

RESEARCH METHODOLOGY

AHP is a decision-making tool having multi-criteria which was initially developed by Prof. T.L. Saaty (1977). This technique is useful in arranging the criteria or factors in a hierarchical structure, comparing the criteria with their relative importance and making decisions and synthesis of interest. In this study, AHP technique is applied by identifying 7 important factors through literature review and by consulting users of social media applications. An AHP questionnaire is formed and filled by 350 social media users of Punjab, Haryana and Chandigarh region. They were explained the procedure of answering AHP based questionnaire and ranking the pair wise comparison of factors, that influence the decision to choose the social media platform, on the basis of its relative importance. Following steps were followed in AHP technique:

Step 1: Identification of various factors through literature review and with the consultation of experts.

Step 2: AHP questionnaire filled from individual investors in pair wise comparison matrix using the scale described by Saaty. The instance scale for the comparison (Saaty & Vargas, 1987):

Scale	**Degree of Preference**
1	Equally Important
3	Moderately Important of one factor over another
5	Strongly or Essentially important
7	Very Strongly important
9	Extremely important
2,4,6,8	Intermediate Values
Reciprocals	For inverse comparisons

Step 3: Normalize the matrix by computing the Normalized Inputs (Priority/Eigen Vector)

Step 4: Consistency of data is checked by calculating Consistency Ratio (CR):

$$\mathrm{CR} = \frac{CI}{RI}$$

Where CI (Consistency Index) calculated as follows:

$$\mathrm{CI} = \frac{\lambda \max - n}{n - 1}$$

And RI is Random Index and value of random index was taken from the following table (Saaty, 1980):

n	1	2	3	4	5	6	7	8	9	10
RI	0.00	0.00	0.58	0.90	1.12	1.24	1.32	1.41	1.46	1.49

Random Index is taken for n=8

Practically, a CR equals to 0.1 or less is considered to be acceptable and assumed that the data is consistent.

DATA COLLECTION AND ANALYSIS

In order to attain the objectives of the study, primary data had been collected from 350 users of social media platform of Punjab, Haryana and Chandigarh region. AHP questionnaire was filled from them as shown below:

AHP Questionnaire

	Third-Party App Permissions	Location Access	Privacy Settings Complexity	Lack of Transparency in Data Practices	Intrusive Advertising	Saved Password	Retention of User Data
Third-Party App Permissions	1						
Location Access	×	1					
Privacy Settings Complexity	×	×	1				
Lack of Transparency in Data Practices	×	×	×	1			
Intrusive Advertising	×	×	×	×	1		
Saved Password	×	×	×	×	×	1	
Retention of User Data	×	×	×	×	×	×	1

Pairwise Comparison Matrix

	Third-Party App Permissions	Location Access	Privacy Settings Complexity	Lack of Transparency in Data Practices	Intrusive Advertising	Saved Password	Retention of User Data
Third-Party App Permissions	1.00	7.32	8.18	6.98	7.20	4.89	8.79
Location Access	0.14	1.00	2.91	0.22	0.31	0.28	6.70
Privacy Settings Complexity	0.12	0.34	1.00	0.20	0.25	0.26	2.01
Lack of Transparency in Data Practices	0.14	4.61	5.03	1.00	0.37	0.29	5.23
Intrusive Advertising	0.14	3.23	4.02	2.72	1.00	0.25	4.30

Saved Password	0.20	3.61	3.91	3.48	3.93	1.00	6.09
Retention of User Data	0.11	0.15	0.50	0.19	0.23	0.16	1.00
Total	1.86	20.27	25.55	14.78	13.29	7.13	34.11

In the Pairwise comparison matrix, mean of all the responses were taken. Then value of each cell was divided by the sum of that respective column to yield its normalised score. The normalised score so derived was put in the Normalisation matrix as follows:

Normalisation Matrix

	Third-Party App Permissions	Location Access	Privacy Settings Complexity	Lack of Transparency in Data Practices	Intrusive Advertising	Saved Password	Retention of User Data	Total	Normalised Principal	Consistency Measure
Third-Party App Permissions	0.54	0.36	0.32	0.47	0.54	0.69	0.26	3.18	0.45	8.85
Location Access	0.07	0.05	0.11	0.01	0.02	0.04	0.20	0.51	0.07	7.05
Privacy Settings Complexity	0.07	0.02	0.04	0.01	0.02	0.04	0.06	0.25	0.04	7.42
Lack of Transparency in Data Practices	0.08	0.23	0.20	0.07	0.03	0.04	0.15	0.79	0.11	8.11
Intrusive Advertising	0.07	0.16	0.16	0.18	0.08	0.04	0.13	0.81	0.12	8.76
Saved Password	0.11	0.18	0.15	0.24	0.30	0.14	0.18	1.29	0.18	9.09
Retention of User Data	0.06	0.01	0.02	0.01	0.02	0.02	0.03	0.17	0.02	7.52
									CI	**0.10**
									RI	**1.41**
									CR	**0.07**

In the above table, Consistency Index (CI) was calculated with the help of following formula:
CI = λ max – n/n-1
λ max=Average of consistency measure
Consistency measures were calculated with the help of Excel's matrix multiplication function.

INTERPRETATION

From the Normalisation Matrix table, it shows that Third-Party App Permissions (with 45% weightage) is the most important factor which influence the decision for selecting Social Media Platform by the social media user, followed by Saved Password with 18% weightage. It is also interpreted that Retention of User Data is least important for the social media use while selecting the social media platform.

Consistency Ratio (CR) is 0.07 as it is less than 0.1 and practically, a CR equals to 0.1 or less is considered to be acceptable. It indicates that the data or preference ratings were consistent.

FINDINGS AND CONCLUSION

There are different factors or concerns of data privacy which may influence the decision for selecting social media platform by an individual. The result of the study indicates that "Third-Party App Permissions", "Saved Password" and "Intrusive Advertising" are the most significant factors or concerns for the users followed by "Lack of Transparency in Data Practices", "Location Access", "Privacy Settings Complexity", and "Retention of User Data". The result and findings may be diverse in the distinctive region. Moreover, there are various other factors which can also be taken that influence the decision of social media platforms. The study provides insights to the Social media app/website developers and to focus on the most important factors or concerns which influence the social media users.

REFERENCES

- Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. Security and Privacy, 2005 IEEE Symposium
- Brignull, H., & O'Brien, J. (2013). Dark patterns: Deception vs. nudging in ux design. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.
- Bernal, P. (2016). Privacy, antiterrorism, and the European convention on human rights after the Charlie Hebdo attack. International Data Privacy Law, 6(1), 18-32.
- Diakopoulos, N. (2016). Accountability in algorithmic decision making: A primer and key challenges. Data Society Research Institute.
- Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2013). Privacy calculus model in e-commerce—a study of Italy and the United States. European Journal of Information Systems, 22(6), 698- 712.
- Dwyer, C., Hiltz, S. R., & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. Proceedings of the Thirteenth Americas Conference on Information Systems.
- Li, E. Y., Wang, Y., Huang, L., & Huang, C. (2014). Prioritizing privacy factors in online social networks: An empirical study. Internet Research, 24(2), 225-243.
- Nentwig, T., & Wozniak, T. (2020). Unpacking platform trust in the sharing economy: Evidence from Airbnb. Technological Forecasting and Social Change, 150, 119780.
- Saaty, T.L. (1980). The analytic hierarchy process. McGraw-Hill: New York.
- Saaty, T.L., & Hu, G. (1998). Ranking by eigenvector versus other methods in the analytic hierarchy process. Pergamon. 11(4), 121-125.
- 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.
- Tsai, J. Y., & Kelley, P. G. (2015). Comprehension and selection behavior of privacy notices online: A comparative study. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.
- Wisniewski, P., & Knijnenburg, B. P. (2017). A framework for understanding and improving online privacy policies. Journal of the Association for Information Science and Technology, 68(12), 2747-2760.
- Xu, H., Dinev, T., Smith, J. H., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. Journal of the Association for Information Systems, 12(12), 798-824.