www.gmcrjournal.com

GMCR
GLOBAL MASS COMMUNICATION REVIEW
communicating humanity

VOL. IX, ISSUE III, SUMMER (SEPTEMBER-2024)

GMCR

GLOBAL MASS COMMUNICATION REVIEW
HEC-RECOGNIZED CATEGORY-Y

Humanity Publications
sharing research
www.humapub.com
US | UK | Pakistan

Article Title

Critical Analysis of the Ethical Challenges related to Data Privacy and Social Media Analytics: A Literature Review

Abstract

The aim of this study is to find out the ethical challenges to social media data privacy because social media plays an information and dissemination role in our society while on the other side, it is also facing data privacy problems. The study analyzed 38 articles related to Facebook and Twitter to explore the viewpoint of the scholars regarding ethical challenges to data privacy linked to social media. The study revealed that social media users are facing data privacy problems and ethical challenges. Both have their own status and requirements regulations, rights, and laws to protect each other from any mishap in society. It is recommended that social media users read and learn all the rules & regulations and conditions whenever logging into a particular Social Network Site, the SNS providers need to clearly define their rules & regulations, and conditions to use to overcome ethical challenges.

Keywords: Critical Analysis, Ethical Challenges, Data Privacy, Social Media Analytics, Literature Review

Authors:

Khayam Hassan: (Corresponding Author)
PhD Scholar, Department of Media and Communication Studies, National University of Modern Languages, Islamabad, Pakistan.
(Email: khayamhasan@gmail.com)

Ayesha Siddiqua: Associate Professor, Department of Media and Communication Studies, National University of Modern Languages, Islamabad, Pakistan.

Waqas Bin Ayaz: PhD Scholar, Department of Media and Communication Studies, National University of Modern Languages, Islamabad, Pakistan.

Citing this Article

06	Critical Analysis on the Ethical Challenges related to Data Privacy and Social Media Analytics: A Literature Review					
	Author	Khayam Hassan Ayesha Siddiqua Waqas Bin Ayaz	**DOI**	10.31703/gmcr.2024(IX-III).06		
Pages		54-61	**Year**	2024	**Volume**	IX	**Issue**	III

Referencing & Citing Styles	**APA**	Hassan, K., Siddiqua, A., & Ayaz, W. B. (2024). Critical Analysis on the Ethical Challenges related to Data Privacy and Social Media Analytics: A Literature Review. *Global Mass Communication Review*, *IX*(III), 54-61. https://doi.org/10.31703/gpsr.2024(IX-III).06
	CHICAGO	Hassan, Khayam, Ayesha Siddiqua, and Waqas Bin Ayaz. 2024. "Critical Analysis on the Ethical Challenges related to Data Privacy and Social Media Analytics: A Literature Review." *Global Mass Communication Review* IX (III):54-61. doi: 10.31703/gpsr.2024(IX-III).06.
	HARVARD	HASSAN, K., SIDDIQUA, A. & AYAZ, W. B. 2024. Critical Analysis on the Ethical Challenges related to Data Privacy and Social Media Analytics: A Literature Review. *Global Mass Communication Review,* IX**,** 54-61.
	MHRA	Hassan, Khayam, Ayesha Siddiqua, and Waqas Bin Ayaz. 2024. 'Critical Analysis on the Ethical Challenges related to Data Privacy and Social Media Analytics: A Literature Review', *Global Mass Communication Review*, IX: 54-61.
	MLA	Hassan, Khayam, Ayesha Siddiqua, and Waqas Bin Ayaz. "Critical Analysis on the Ethical Challenges Related to Data Privacy and Social Media Analytics: A Literature Review." *Global Mass Communication Review* IX.III (2024): 54-61. Print.
	OXFORD	Hassan, Khayam, Siddiqua, Ayesha, and Ayaz, Waqas Bin (2024), 'Critical Analysis on the Ethical Challenges related to Data Privacy and Social Media Analytics: A Literature Review', *Global Mass Communication Review,* IX (III), 54-61.
	TURABIAN	Hassan, Khayam, Ayesha Siddiqua, and Waqas Bin Ayaz. "Critical Analysis on the Ethical Challenges Related to Data Privacy and Social Media Analytics: A Literature Review." *Global Mass Communication Review* IX, no. III (2024): 54-61. https://dx.doi.org/10.31703/gpsr.2024(IX-III).06.

Global Mass Communication Review

www.gmcrjournal.com

DOI: http://dx.doi.org/10.31703/gmcr

GMCR

Title

Critical Analysis on the Ethical Challenges related to Data Privacy and Social Media Analytics: A Literature Review

Authors:

Khayam Hassan: (Corresponding Author)
PhD Scholar, Department of Media and Communication Studies, National University of Modern Languages, Islamabad, Pakistan.
(Email: khayamhasan@gmail.com)

Ayesha Siddiqua: Associate Professor, Department of Media and Communication Studies, National University of Modern Languages, Islamabad, Pakistan.

Waqas Bin Ayaz: PhD Scholar, Department of Media and Communication Studies, National University of Modern Languages, Islamabad, Pakistan.

Abstract

The aim of this study is to find out the ethical challenges to social media data privacy because social media plays an information and dissemination role in our society while on the other side, it has also faced data privacy problems. The study analyzed 38 articles related to Facebook and Twitter to explore the viewpoint of the scholars regarding ethical challenges to data privacy linked to social media. The study revealed that social media users are facing data privacy problems and ethical challenges. Both have their own status and requirements regulations, rights, and laws to protect each other from any mishap in society. It is recommended that social media users read and learn all the rules & regulations and conditions whenever logging into a particular Social Network Site, the SNS providers need to clearly define their rules & regulations, and conditions to use to overcome ethical challenges.

Contents:

Introduction

This study aims to assess the social media data privacy ethical challenges from the perspective of different research scholars to find out the problems and challenges to the uses and providers of Social Network Sites. Marín et al. (2022) examined the relationship between education, data privacy, and social media. Pre-service teachers from four different nations participated in the worldwide

comparative study, which found a mixed bag of worries about data privacy and optimism about social media's educational possibilities. The study made clear how important it is for instructors and students to adopt more data privacy-related behaviors and understanding, taking into account the cultural and legal contexts of various nations.

Dhiman (2021) said that one of the key ethical problems of large-scale data collecting via social media is the issue of permission. Users of social media networks should understand how their data is gathered and utilized. Lack of awareness might result in consumers unintentionally consenting to data management practices. Companies and organizations collecting substantial amounts of data must acquire informed consent from users and explain how their data will be used.

Mitchell and El-Gayar (2020) conducted a comprehensive literature study from 2006 to 2021, examining 33 studies that investigated privacy problems in online social networks. Their findings highlighted consumers' concerns about identity theft, data leakage by third-party applications, and the degree of control they have over their information. To address these issues, strategies such as encryption and authentication were offered; nonetheless, users frequently underutilize existing privacy policies and settings.

Castells (2009) stated that misinformation and false records have enormous consequences, inclusive of detrimental democratic methods and placing public health at risk. Another concern is cyberbullying, which can cause intellectual fitness difficulties or even suicide. Moreover, social media may be addicting and have a harmful effect on mental health, particularly for those who use it often. Dhiman, (2022) explored that people ought to use social media well and recognize its dangers and moral implications. With the aid of making use of social media intelligently and ethically, we are able to all make contributions to creating more secure and greater high-quality online surroundings.

In the digital world of today, the widespread usage of social media platforms has resulted in massive amounts of data. This data contains personal information such as user demographics, interests, and habits (Banu, 2019). The use of this data for social media analytics raises various ethical concerns, notably those related to data privacy. Privacy is a fundamental principle that individuals should have control over their personal information. One of the most significant ethical issues in data privacy and social media analytics is the acquisition and use of personal information without the individual's informed consent or understanding. This raises worries about the possibility of data breaches, identity theft, and illegal access to personal information (Iaccarino, 2015).

According to Infosys BPM (2024), social media and e-commerce usage have increased dramatically over the last decade, as has observation and intrusion into people's lives. The majority of people have encountered privacy attacks on the internet. According to a 2017 Statista poll of persons aged 18 to 29, 20% passed up potential employment prospects, 48% purchased without intending to, and 56% had links, comments, or posts read by unintended people. People join online communities to communicate with people who share similar interests. Such forums and social media are used to share information, opinions, and, unknowingly, attitudes and habits.

In step with Cariblogger.com (20108) social networking offerings like Facebook, Instagram, Twitter, and LinkedIn have millions of followers and customers. They actively post and disseminate fabric on social media in fractions of a second. The advantages of those new technologies, together with more desirable openness and public engagement, need not be left out. Capability negatives encompass the veracity of statistics, the authenticity of the uploaded cloth, and source, and the lengthy-term presence of defective information. Because of a lack of awareness about the dangers of social networking, energetic clients are visible and reachable through their profile pages, which encompass non-public statistics inclusive of vicinity and contact amount. These customers are much more likely to be publicly targeted. Moreover, the boom of mobile devices, along with web-primarily based cellular telephones, permits the on-the-spot capture of statistics. In spite of its sensible and beneficial ability for social and developmental increase in human communication, social networking raises several ethical concerns that should be addressed.

Objectives

- ▪ To find out the viewpoints of the scholars regarding data privacy related to social media sites and ethical challenges
- ▪ To explore the perspective of scholars regarding the ethical standards, rules & regulations, and conditions of the users and providers

Research Question

1. What kinds of ethical standards, rules & regulations, and conditions are faced by users and providers of Social Network Sites?

Method and Materials

The researchers analyzed articles, collected from different research journals and Google Scholar through the search terms i.e. social media analytics, data privacy, ethical standards, ethical challenges, rules, & regulations, and conditions. The researcher collected 70 articles while reviewing 38 articles in this study because the others were not more related to the aim of the study. Each of the articles was carefully analyzed and then draws a conclusion, which was mentioned in the literature review. Discussion and conclusion were done on the basis of that analysis.

Studies on Facebook and Twitter

Although social media analytics has completely changed networking and communication, it also brings up moral questions. Due to social media platforms' access to user data, privacy issues and inquiries concerning the storage, collection, and use of this data have surfaced. (Dhiman, 2023b), Monell, 2023, Liu, 2023). There are worries regarding the storage, collection, and use of personal data because social media platforms have access to a large amount of it. Users should understand the dangers of disclosing private information on social media. On social media, fake news may travel swiftly and have harmful effects. Social media posts and false information have the power to sway people's opinions and decisions. It will need a responsible and ethical attitude from people and society as a whole to solve these ethical issues in the media (Dhiman, 2023). The advancement of technology and the popularity of social media have exposed private users to risks such as user profiling, sensitive marketing, and

fraud. A balance must be struck between the development of information technology and the protection of personal privacy. The article argues that people, platforms, and governments must work together to protect privacy (Jin, 2023).

This study investigates the perceptions of pre-university teachers in Germany, New Zealand, Spain, and the United States regarding the educational and professional use of social media and its speed privacy, and application. The results show that while there is a general belief in the educational potential of social media, there are still concerns about data privacy and a lack of knowledge about data privacy. Differences exist between participants from different universities, indicating that cultural values, legal norms, and user behavior play a role in pressures to access social media profile privacy. These findings demonstrate the need for further research and implications for practice and policy regarding the handling of personal information in the use of social media in education. Research also shows that New Zealand pre-service teachers are more willing to take on the responsibility of teaching technology content to students than their counterparts in the United States and Germany (.

Privateness risks on social media platforms maintain growth because of the increase of new platforms and customers. Default privateness regularly leaves customers at risk of online tracking, intelligence accumulating, and identity theft. Privacy on social media structures is superb, but using them correctly may be hard. Studying systems like virtual-pass and open-source gear like SocialScore can help users conquer privacy weaknesses by gambling video games and producing reports on nice practices in cybersecurity. This examination centered on the three maximum popular social media structures inside the USA (FB, Instagram, Twitter), however, Destiny Research must have a look at popular social media websites out of doors in the US, as well as sites that are much less famous among customers. Digital bypass and SocialScore have been validated to be realistic and possible answers to social privateness troubles (Virpi, Kristiina, Tuunainen., Olli, Pitkänen., Marjaana, Hovi. 2009).

Most people do not read the license, do not understand the service, and do not agree when they

see it. Many elites will support other models, such as private payments or the sale of personal data. Different generations differ in how they value their information. The findings show that there are concerns about privacy and the potential for information to be disclosed to unsuspecting recipients, but misunderstandings persist about the use of text information from service providers. The paper presents findings comparing people's support, or lack thereof, to various activities related to data use and privacy rights. Research results show that different generations have different attitudes and behaviors toward personal data and the use of personal data by service providers. This article also highlights the importance of understanding and analyzing the content of services offered through social media, such as Twitter and Google (Brito et al., 2013).

Chinese people's online information in public areas has inadequate privacy protections, such as friend updates and age information. Women are more sensitive to personal information, but there is no protection technology and there is no change in special measures to protect identity. Men, on the other hand, are often careless and lazy when it comes to self-defense. Both men and women lack the understanding of privacy protection, such as encryption technology, electronic technology, security authentication, and digital encryption technology (Zhao & Dong, 2017).

The popularity of social networking sites has led to many social and ethical problems, especially the privacy problems of SNS members. A survey was conducted of 100 university students in Malaysia to examine their knowledge of self-protection and social networking use. The results of the survey show that most students are aware of self-regulation on SNS. But less than half change or update these settings. The results of this survey are crucial to understanding how users protect themselves and may inform the improvement of future privacy protection (Keng, Yew, Lau., Ming, Ma., Wai, Hong, Mak., Nasriah, Zakaria.) 2011.

Misinformation is created and disseminated on social media, bringing attention to problems with techniques of detection, response, and prevention. It displays the quick expansion of social media platforms and their potency in thwarting false information, such as fake news and phishing

websites. To comprehend its effects and guide future research in this field, the essay highlights the necessity of looking into disinformation on social media (Wu et al., 2016).

Fake news spreading on social media presents another difficulty as it will have far-reaching effects and influence people's opinions and judgments (Mahoney et al., 2023). Information society ethics: user identification disclosure, privacy, conditions of use for sharing and producing information, and so on. In the context of migration, social research has given rise to new ethical concerns about analysis, permission, and anonymity, particularly for people for whom the support system is inadequate. These are ethical difficulties that researchers need to consider.

Strict action must be taken against users who use fake information and make people seem bad, emphasizing the significance of government privacy and security measures (Bala, 2022).

An organization's reputation and revenue can suffer greatly from poor data security, particularly in e-commerce where customers may be harmed by security flaws. It draws attention to the shortcomings of pseudonymization software and the requirement for further security measures in order to safeguard private data. In order to prevent counterfeit shipments, further security measures are required to safeguard information confidentiality (Rossi et al., 2022).

Throughout all classes of information, fake news is more massive, quicker, deeper, and broader than actual news. Political fake news has an extra impact on communication than fake news approximately terrorism, herbal failures, technology, urban legends, or monetary statistics. Faux information is seen as more common than actual information, making humans more likely to participate. Actual stories inspire wish, sadness, pleasure, and trust in reactions, even as faux memories inspire fear, hatred, and curiosity. Unlike traditional intelligence, bots and humans report true and false news just as quickly, suggesting that humans are more likely to report fake news (Vosoughi et al., 2018). An extensive analysis of social media fake news detection is presented in this study, along with examples of false news based on social theories and psychology, assessment metrics, and available data mining methods. The

text delves into the difficulties and distinctive features of identifying false information on social media platforms. These include the deliberate fabrication of false material to deceive readers and the requirement for additional data, which includes social media interactions with customers, so one can reach conclusions. With an intensive evaluation of the problem and discussions of applicable look areas, unresolved issues, and future research paths, the poll seeks to aid greater research into the detection of fake news on social media (Shu et al., 2017).

Whilst social media was regarded as the "maximum essential" source of election information by 14% of Americans, it has become now not the number one supply. On Facebook, fake records supporting Trump were shared 30 million times, however fake facts assisting Clinton were shared eight million times.

In the months leading up to the election, the everyday grownup American viewed one or more fake news objects; of folks who remembered viewing them, slightly greater than half stated they believed them. Tales that guide a candidate they like are more likely to be believed by the public, specifically if those humans have social media networks with exclusive ideologies (Allcott & Gentzkow, 2017). This look identified 3 privacy troubles on social networking websites (SNS) including MySpace, FB, and LinkedIn. SNSs offer privacy that cannot be effortlessly changed to defend customers' records, and customers haven't any manage over the facts others share approximately them. This newsletter introduces privateness as a framework for solving privacy problems in SNS (Ai, Ho., Abdou, Maiga., Esma, Aämeur. 2009). The examine surveyed 210 Facebook customers and found that most individuals disclosed a number of private facts on the platform, despite the fact that they were no longer sure that their facts may be seen with the aid of unknown events. Individuals lack information and know-how about Facebook's privacy policy and terms of use (Virpi, Kristiina, Tuunainen., Olli, Pitkänen., Marjaana, Hovi. 2009). Privacy concerns are not a strong determinant of whether people will join the Facebook social network. Privacy-conscious individuals will also join networks and share more personal information depending on the information they provide and whether they can

control outside access to that information. Members have misconceptions about the size and mix of online communities and the visibility of their profiles. Age, education, and Internet experience were associated with Facebook participation. Non-members are attracted to online social networks such as Facebook due to privacy concerns (Acquisti & Gross, 2006). Similar levels of privacy concerns were reported by 4,444 Facebook and MySpace members. Facebook members trust Facebook and its members more and are willing to share personal information. MySpace members report improved experiences using the site to meet new people. Trust is not as necessary when forming new relationships in online dating as it is when meeting face to face. The existence of trust and willingness to share information does not translate into new relationships on online sites. Online relationships can develop on websites where trust is strong and privacy protection is weak (Catherine, Dwyer., Starr, Roxanne, Hiltz., Katia, Passerini. 2007). Facebook is integrated into users' daily lives with special processes and performances that show that it is used and important to users. Users who claim to be aware of privacy concerns are still uploading more personal data which demonstrates the potential impact of information and behavior. Users often comment on psychological effects similar to the third-party effect, taking further privacy risks for themselves. Users who have experienced a privacy breach are more likely to change their privacy settings than users who have only heard of a privacy breach from others; This suggests that there is awareness of the individual's role in self-management. Safe use of social media requires a change in user behavior that leads to a combination of interest, usage patterns, and side effects. Three (Debatin et al., 2009).

The research focuses on automated approaches to tweet credibility assessment for "trending" subjects. To determine whether a tweet is genuine or not, the authors analyze aspects gleaned from users' posting and re-posting habits, the post's content, and references to other sources. It is possible to classify tweets automatically with precision and recall in the range of 70% to 80% based on quantifiable variations in the propagation of messages, as demonstrated by the evaluation of their approaches using human evaluations. The identical news title was judged to be far less

trustworthy by users on Twitter than it was on blogs or traditional media websites, according to a prior experiment that is included in the research (Castillo et al., 2011).

There is a significant difference in the disclosure of private and public information on Twitter, indicating that private information behaves differently than public information. Privacy policy has been proposed to reduce the disclosure of private information in social networks (Hu et al., 2023).

Public and private information are dispersed differently, and social media provides a Twitter dataset for study on this topic. Additionally, it offers privacy-preserving measures to reduce the spread of privacy (Hu et al., 2023b). Fraud, user profiling, and precision marketing are the three scenarios in which user privacy is vulnerable. The statement underscores the need to strike a balance between the advancement of information technology and safeguarding individual privacy. The study makes privacy protection recommendations while emphasising the value of cooperation between users, platforms, and governments (Jin, 2023)User-defined control levels over personal information are possible with a new kind of privacy policy known as a data handling policy. Guidelines for data management specify how the receiving party will handle the release of personal information. These rules are designed to protect user privacy by making sure that personal data that is gathered for one reason isn't utilized for another without the individual's express, informed permission. According to the study, it is crucial for users to be in charge of what information about them is visible to whom and when ((Ardagna et al., 2006).

Using sticky rules and tracking services based on identity-based encryption (IBE) and TCPA technology, this novel strategy protects users' privacy and increases organizational accountability. The paradigm and technology solution outlined in the article address the issues of increasing user control over privacy and personal data as well as holding businesses more responsible for their actions. In order to improve accountability, keep users informed about disclosures, and stop information from being disclosed without authorization, the system makes use of IBE technology and a TA service infrastructure. For proactive security and trust assessments, TCPA technology is employed (Mont et al., 2004).

Discussion and Conclusion

The discussion on privacy risks associated with social media platforms underscores the growing concerns amidst the proliferation of new platforms and users. Default privacy settings often leave users susceptible to online tracking, intelligence gathering, and identity theft. Despite the challenges, efforts to enhance privacy are underway, with learning platforms like Digital-PASS and open-source tools like SocialScore offering valuable resources to empower users in navigating cybersecurity best practices. While this study focused on popular social media platforms in the United States, there is a call for future research to extend its scope to encompass global platforms and lesser-known platforms. Insights from the study highlight the nuanced generational differences in attitudes toward privacy and data use, underscoring the need for tailored approaches to address privacy concerns. Additionally, the findings emphasize the importance of scrutinizing the terms of service and understanding the implications of data usage by service providers. This discourse serves as a crucial step towards fostering a more informed and proactive approach to safeguarding privacy in the digital age.

The researchers highlighted the consumers' worries regarding identity theft, third-party data leaks, and the level of control over their personal information. Despite proposed solutions such as encryption and authentication, users often neglect to fully utilize available privacy settings and policies. Privacy concerns on social networking sites (SNS) like Facebook are paramount, as users often disclose personal information without a full understanding of privacy policies or control over their data. Studies indicate that while trust plays a role in sharing personal information online, it does not always translate into meaningful relationships. These findings emphasize the need for improved privacy education and control mechanisms to ensure the safe and responsible use of social media platforms.

References

Acquisti, A., & Gross, R. (2006). Imagined communities: awareness, information sharing, and privacy on Facebook. In *Lecture notes in computer science* (pp. 36–58). https://doi.org/10.1007/11957454_3
Google Scholar   Worldcat   Fulltext

Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 election. *The Journal of Economic Perspectives*, *31*(2), 211–236. https://doi.org/10.1257/jep.31.2.211
Google Scholar   Worldcat   Fulltext

Ardagna, C. A., De Capitani Di Vimercati, S., & Samarati, P. (2006). Enhancing user privacy through data handling policies. In *Lecture notes in computer science* (pp. 224–236). https://doi.org/10.1007/11805588_16
Google Scholar   Worldcat   Fulltext

Bala, R. (2022). Challenges and ethical issues in data privacy. *International Journal of Information Retrieval Research*, *12*(2), 1–7. https://doi.org/10.4018/ijirr.299938
Google Scholar   Worldcat   Fulltext

Banu, S, S & Kavitha, G., (2019) Analysis of User Perception using Twitter Data, *International Journal for Research in Applied Science & Engineering Technology*, Volume 7 Issue V.
Google Scholar   Worldcat   Fulltext

Brito, K. D. S., Garcia, V. C., Durao, F. A., & De Lemos Meira, S. R. (2013). How people care about their personal data released on social media. . https://doi.org/10.1109/pst.2013.6596044
Google Scholar   Worldcat   Fulltext

Castells, M. (2009). *Communication power*. Oxford University Press.
Google Scholar   Worldcat   Fulltext

Castillo, C., Mendoza, M., & Poblete, B. (2011). Information credibility on Twitter. .https://doi.org/10.1145/1963405.1963500
Google Scholar   Worldcat   Fulltext

Debatin, B., Lovejoy, J. P., Horn, A., & 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
Google Scholar   Worldcat   Fulltext

Dhiman, B. (2023). Ethical Issues and Challenges in Social Media: A Current Scenario. .https://doi.org/10.20944/preprints202303.0513.v1

Google Scholar   Worldcat   Fulltext

Dhiman, B. (2023b). Ethical Issues and Challenges in Social Media: A Current Scenario. .https://doi.org/10.36227/techrxiv.22662844
Google Scholar   Worldcat   Fulltext

Dhiman, D. (2021). Psychosocial Impact of Web Series and Streaming Content: A Study on Indian Youth. *Global Media Journal 19*(46:281):1-7.
Google Scholar   Worldcat   Fulltext

Dhiman, D. (2022). Condition of Women Prisoners in Model Jail, Chandigarh: A Communication Study. *International Journal of Psychosocial Rehabilitation 26*(1):23-34.
Google Scholar   Worldcat   Fulltext

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 2007 International Conference on Information Systems (ICIS)*, 1-10.
Google Scholar   Worldcat   Fulltext

Ho, A., Maiga, A., & Aimeur, E. (2009). Privacy protection issues in social networking sites. . https://doi.org/10.1109/aiccsa.2009.5069336
Google Scholar   Worldcat   Fulltext

Hu, X., Zhu, T., Zhai, X., Zhou, W., & Zhao, W. (2023b). Privacy Data propagation and preservation in social media: a Real-World case study. *IEEE Transactions on Knowledge and Data Engineering*, *35*(4), 4137–4150. https://doi.org/10.1109/tkde.2021.3137326
Google Scholar   Worldcat   Fulltext

Iaccarino, G. (2015). A look at internet privacy and security issues and their relationship to the electronic job search: Implications for librarians and career services professionals. *The Reference Librarian, 26*(55), 107–113.
Google Scholar   Worldcat   Fulltext

Infosys BPM. (2024). *Data privacy and ethical considerations in web and social media analytics*. https://www.infosysbpm.com/blogs/web-social-analytics/data-privacy-and-ethical-considerations-in-web-and-social-media-analytics.html
Google Scholar   Worldcat   Fulltext

Jin, J. (2023). "Taking Down the Monitoring": Privacy protection for social media user in the era of big data. *Lecture Notes in Education Psychology and Public Media*, *5*(1), 111–118. https://doi.org/10.54254/2753-7048/5/20220424
Google Scholar   Worldcat   Fulltext

Keng, Y. L., Ma, M. W., Mak, H. W., & Zakaria, N. (2011). A study on privacy concerns in social networking sites (SNS). *CORE.* https://core.ac.uk/outputs/42980872/?source=4 Google Scholar   Worldcat   Fulltext

Mahoney, J., Louvier, K. L., & Lawson, S. (2023). The Ethics of Social Media Analytics in Migration Studies. *arXiv (Cornell University).* https://doi.org/10.48550/arxiv.2302.14404 Google Scholar   Worldcat   Fulltext

Marín, V. I., Carpenter, J. P., Tur, G., & Williamson-Leadley, S. (2022b). Social media and data privacy in education: an international comparative study of perceptions among pre-service teachers. *Journal of Computers in Education*, 10(4), 769–795. https://doi.org/10.1007/s40692-022-00243-x Google Scholar   Worldcat   Fulltext

Mitchell, D., & El-Gayar, O. (2020). The Effect of privacy policies on information sharing behavior on social networks: A Systematic literature review. *Proceedings of the . . . Annual Hawaii International Conference on System Sciences/Proceedings of the Annual Hawaii International Conference on System Sciences.* https://doi.org/10.24251/hicss.2020.517 Google Scholar   Worldcat   Fulltext

Mont, M., Pearson, S., & Bramhall, P. (2004). Towards accountable management of identity and privacy: sticky policies and enforceable tracing services. https://doi.org/10.1109/dexa.2003.1232051 Google Scholar   Worldcat   Fulltext

Rossi, A., Arenas, M. P., Kocyigit, E., & Hani, M. (2022). Challenges of protecting confidentiality in social media data and their ethical import. . https://doi.org/10.1109/eurospw55150.2022.00066 Google Scholar   Worldcat   Fulltext

Shu, K., Sliva, A., Wang, S., Tang, J., & Liu, H. (2017). Fake news detection on social media. *ACM SIGKDD Explorations Newsletter*, 19(1), 22–36. https://doi.org/10.1145/3137597.3137600 Google Scholar   Worldcat   Fulltext

Virpi, K., Tuunainen, O., & Hovi, M. (2009). Users' awareness of privacy on online social networking sites: Case Facebook. Google Scholar   Worldcat   Fulltext

Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science*, 359(6380), 1146–1151. https://doi.org/10.1126/science.aap9559 Google Scholar   Worldcat   Fulltext

Wu, L., Morstatter, F., Hu, X., & Liu, H. (2016). Mining Misinformation in Social Media. 135–162. https://doi.org/10.1201/9781315396705-14 Google Scholar   Worldcat   Fulltext

Zhao, H., & Dong, H. (2017). Research on personal privacy Protection of China in the era of Big Data. *Open Journal of Social Sciences*, 05(06), 139–145. https://doi.org/10.4236/jss.2017.56012 Google Scholar   Worldcat   Fulltext