Khizanah al-Hikmah : Jurnal Ilmu Perpustakaan, Informasi, & Kearsipan
p-ISSN: 2354-9629
e-ISSN: 2549-1334
Volume 12 Issue 1, June, 2024

Comparison of Data Security and User Privacy on Instagram and Twitter: A Literature Study

Arly Maya Berlyanti Dwi Santoso[1], Eva Alisya Febrianti[2], & Fitri Mutia[3]

[1,2,3]Universitas Airlangga, Indonesia
Correspondence email: arly.maya.berlyanti-2022@fisip.unair.ac.id

Information

Submitted: 25-01-2024
Revised: 18-02-2024
Accepted: 04-05-2024

How to cite: Dwi Santoso, A. M. B., Eva Alisya Febrianti, & Fitri Mutia. (2024). Comparison of Data Security and User Privacy on Instagram and Twitter: A Literature Study. Khizanah Al-Hikmah : Jurnal Ilmu Perpustakaan, Informasi, Dan Kearsipan, 12(1). https://doi.org/10.24252/kah.v12i1a7

DOI: 10.24252/kah.v12i1a7

ABSTRACT

This comprehensive literature study examines and compares data security and user privacy features on social media platforms such as Instagram and Twitter. The method used is a literature study of 25 journal articles from various trusted sources, such as Scopus, ScienceDirect, and Web of Science, with a qualitative approach. The study reveals that Instagram has advantages in some aspects of data security and privacy compared to Twitter. However, both platforms have weaknesses that users should be aware of, including the risk of phishing and cyberattacks. The research also highlights the importance of individual awareness and the implementation of effective data security measures, such as two-factor authentication and strict privacy settings. Although the study provides valuable insights, there are limitations in data collection methods that rely on electronic sources, which may not cover all relevant literature. Therefore, future research is expected to overcome these limitations and provide more up-to-date recommendations for improving data security and user privacy on social media.

Keywords: Data security; user privacy; social media; security threats

1. INTRODUCTION

As reported through the We Are Social page, social media users as of 2023 will reach 4.76 billion worldwide, equivalent to 60% of the total global population. In Indonesia, as of January 2023, social media users will reach 213 million of Indonesia's total population at the beginning of 2023 (We Are Social, 2023). With so many social media users, it certainly does not make Indonesia avoid various problems. Often, the problems that arise are always related to personal data leakage caused by third parties, and most data will be misused for negative things.

Based on We Are Social & Hootsuite (2021), it was found that 64% of the entire Indonesian population is connected to the internet. This is considered if it does not rule out the possibility for third parties to access illegally so that there is the potential for data leakage. According to data from the Indonesian Consumer Institution Foundation (YLKI), in 2019, there were 106 cases of data theft in the banking sector. Meanwhile, on May 21, 2021, news of the

leak of personal data occurred again in Indonesia with as many as 279 million victims, and the data was successfully sold on the "Raid Forums" (https://www.aa.com.tr). Additionally, the Indonesian National Police recorded 1409 fraud cases caused by the leakage of personal data from social media users.

When viewed through Hoosuite.com data as of January 2021, Indonesia's number of Instagram users reached 85 million. Meanwhile, Napoleon Cat reported that in October 2021, Instagram users in Indonesia recorded 91 million. From the two data above, there was a significant increase in the number of users from Instagram users, which was as much as 6 million within 9 months. The large increase in social media users has caused concerns about data security and user privacy in Indonesia and the possibility of personal data leakage to third parties.

Data security and privacy are needed by social media users because these two things are a unity that holds full control over all personal information. All information attached to oneself is sensitive and should not be spread illegally because it can be misused, leading to negative things. If based on facts, many Indonesians, especially social media users, are still not fully aware of the importance of maintaining the confidentiality and security of their data. The use of social media is also not recommended excessively, especially in accessing new things that can endanger the security of personal data.

Social media is one of the social networking sites that users can use for all forms of communication or exchanging information. Based on Boyd & Ellison's (2007) opinion, in its function as a means of exchanging information, social media is divided into several groups, including blogs and microblogs such as Twitter and social networking sites such as Instagram and other social media. Social media has many types, which almost have the same function: sharing information to interact with each other. With so many types of social media available, this paper only focuses on reviewing literature whose focus of writing is only on Instagram and Twitter social media. Both of these social media are quite popular among the general public. With its ability to expand social networks, Instagram and Twitter can attract the general public to use the application continuously and disseminate various information.

In addition, social media can only function properly if users have registered an account and first input personal information and data, such as name, gender, email address, and phone number. With the increase in users, more information and personal data are collected. Thus, risks that can threaten users, especially regarding data security and privacy in social media, are increasing. Issues related to data security and user privacy are important to pay attention to. Various negative impacts, such as identity theft, the spread of false information, and even cyberattacks, result in users understanding the nature of social media use well.

Data security and privacy have become crucial to maintaining information and data privacy. Various efforts have been made through data security measures that users can understand and carry out. Such as compiling unique passwords, activating Two Factor Authentication (2FA), and connecting other social media accounts. Knowing that as social media is a social networking service, problems, and even data security and privacy crimes will still arise when the system continues to run.

According to Moallem, users' understanding of risk and how to protect themselves from cyberattacks is fundamental in modern life (Bhatnagar & Pry (2020). Various content used on social media can also pose a risk of data security threats. However, this is also inseparable from user negligence, where they often accidentally and unknowingly press certain links that lead to fake URLs, which then, on the fake URLs, users are directed to provide confidential information such as usernames and passwords. Another common threat is the spread of malware that can damage the device system, resulting in information leakage. Based on previous research findings, it was found that the cause of cyber security problems is usually the user himself. Therefore, in this case, individual consciousness becomes the most important thing.

This paper addresses the following research questions, with the data gathered from electronic databases, specifically electronic journals. Consequently, the research question examined how data security and privacy levels compare between Instagram and Twitter. Accordingly, this article intends to perform a literature review comparing the data security and privacy of Instagram and Twitter, serving as a foundation for future research. The significance of this study lies in its potential to inform users about the relative safety of their personal information on these platforms and to guide developers in enhancing security measures.

2. METHODS

This research was conducted using a qualitative approach, namely a literature study. Through analysis of relevant literature, this method increases understanding of social media data security and privacy issues. Data were collected from various literature, such as books, journals, and scientific papers, and then selected to identify patterns found in those literature sets. In this study, the author obtained three works of literature on the same topic. The research is written by academic standards, such as citing and respecting the copyright of reference sources. Research may have limitations because data discovery may not include all reference sources, so bias may occur.

Table 1. Research strategy

No.	Database	Keywords
1	Scopus	"privacy and security" AND "social media" AND "case study"
2	Web of Science	"security and privacy" AND ("Twitter" AND "Instagram" OR "social media")
3	Google Scholar	"security and privacy" AND "social media"
4	Sage Journal	"security and privacy" AND "social media" AND "Instagram" AND "Twitter"
5	IEEE	security and privacy of Twitter and Instagram
6	Science Direct	comparing user privacy and data security on social media
7	Research Gate	social media security and privacy

This study implements the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) flow diagram illustrating the selection of studies for the present systematic review based on research by Abhinav et al. (2023).

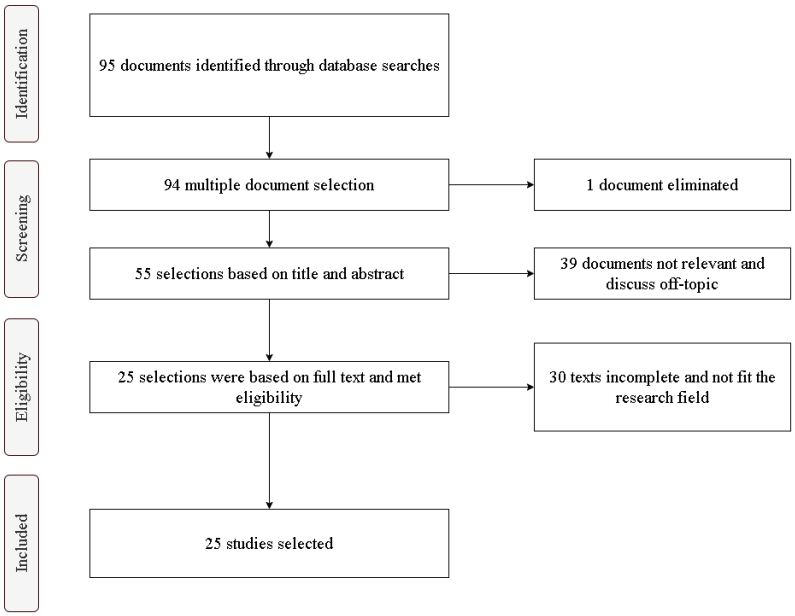

Figure 1. Data selection process with the PRISMA model

The databases used to obtain journal articles include Google Scholar, Scopus, Web of Science, IEEE, Sage Journal, ScienceDirect, and Research Gate. This data was collected from several articles on data security and privacy on Instagram and Twitter from 2007 to 2023. After finding relevant journal articles, the author carries out a process of eliminating information to find out the quality, relevance, and state of information contained in scientific papers. 95 articles that the author managed to find. After selection through the abstract presented, the author gets a scientific article for data analysis. The results of an in-depth analysis of the author's scientific work will be interpreted and re-elaborated using descriptions and tables to provide a clear and structured understanding. Presenting the results in the form of paragraphs and tables simultaneously will provide a comprehensive understanding and effectively convey this research's results to readers.

3. RESULTS AND DISCUSSION

Results

The development of the internet and communication technology also accompanies various kinds of innovations from new sources of information that are friendly to users. Various uses of the internet in fulfilling information have been widely done by users, especially on social media. The number of social media users who experience an increase in numbers from time to time shows that social media is considered capable of meeting the information needs of its users. The widespread use of social media makes it often found problems that cause many negative impacts. Identity theft, data misuse, and even phishing and malware attacks can cause a lot of harm to victims of social media crime. In social media, all data collected into one can be exploited if it is in the wrong hands. However, some users are less concerned about data security and the privacy of their data that has entered the system of social media platforms. Research by Hafidz et al. (2017) has found that the average social media user is a student in the category of teenagers who use their rest and sleep time for the internet and browsing through Instagram. In addition to Instagram, Twitter has skyrocketed in users because of its role in displaying trend information. According to Mistry (2011), Twitter is a social networking service that allows users to share real-time information by posting their experiences and thoughts. Even though there have been many negative impacts that are seen

directly, such as threats, dissemination of personal photos, misuse of personal identity, and so on.

From various scientific articles that have become a reference for this research, 25 suitable research articles were found. The following data findings are described in the table below.

Table 1. Previous research data

No.	Title	Author	Year	Result
1	History of Information: The case of Privacy and Security in Social Media	Dimitris Gritzalis, Miltiadis Kandias, Vasilis Stavrou, and Lilian Mitrou	2014	Instagram and Twitter offer user privacy settings to control who can see their content, but users are often unaware that the information shared could pose a threat.
2	Social Networking Privacy-Who's Stalking You?	Diane Gan and Lily R. Jenkins	2015	On Twitter, users must actively change settings to protect their privacy. Instagram introduced two-factor authentication and allowed users to set their accounts to private.
3	Detecting Anomalies in Twitter Stream for Public Security Issues.	Flora Amato, Giovanni Cozzolino, Antonino Mazzeo and Sara Romano	2016	The Twitter application still needs many additional features to detect various dangerous events, especially crime or user security.
4	Social Function: Integrating Twitter and Instagram for Event Monitoring.	Prasanna Giridhar, Shiguang Wang, Tarek Abdelzaher, Tanvir Al Amin, Lance Kaplan	2017	Instagram is safer than Twitter. This can be seen from the location access provided by Instagram by 15% and Twitter by 1.5%. So it can be concluded that Instagram pays more attention to the security of its users.
5	An Assessment Cram on Security Issue of Fake Identity Behavior in Social Media	Deepak Dashora and Ashok Kumar Jetawat	2017	Instagram and Twitter are equally vulnerable to creating fake identities, such as names, ages, genders, locations, email addresses, and contact numbers to deceive other users.
6	Security Issues in Social Media: Challenges and Solutions	Mardin A. Anwer, Rina Dinkha Zarro, and Kamaran Hama Ali Faraj	2017	Both platforms Instagram and Twitter are equally vulnerable to security threats, such as identity theft and the creation of fake accounts because there are not adequate authentication and authorization checks in place.
7	Why do College Students Prefer Facebook, Twitter or Instagram? Site Affordances, Tensions Between Privacy and Self-Expression, and Implications for Social Capital	Christina Shane-Simpson, Adriana Manago, Naomi Gaggi, Kristen Gillespie-Lynch	2018	Instagram is safer than Twitter. This shows that Instagram users are more likely to choose this platform because of its visual features. Twitter users tend to be individualistic and more likely to set their profiles public.
8	Impact of User Awareness, Trust, and Privacy Concern on Sharing Personal Information on Social Media	Valentinus Paramarta, Muhammad Jihad, Ardhian Dharma, Ika Chandra Hapsari, Puspa Indahati Sandhyaduhita, Achmad Nizar Hidayanto	2018	From this research, it was found that Instagram is safer than Twitter.
9	Rise of spam and compromised accounts in online social networks: A state-of-the-art review of different combating approaches	Ravneet Kaur, Sarbjeet Singh, Harish Kumar	2018	Twitter has its ever-evolving detection methods and tools to address security issues. Meanwhile, Instagram as part of the Facebook ecosystem utilizes the "Facebook Immune System".

10	Improve the Security of Social Media Accounts	Ruslan Shevchuk and Yaroslav Pastukh	2019	Instagram provides reporting tools for users to report suspicious activity or content that violates our community guidelines.
11	Effects of privacy policy visualization on users' information privacy awareness level The case of Instagram	Aikaterini Soumelidou and Aggeliki Tsohou	2019	Instagram already enforces a social media privacy policy by providing necessary information about data collection and use, but many users tend to avoid reading it.
12	Enhancing Social Networking in Smart Cities: Privacy and Security Borderlines	Vaia Moustaka, Zenonas Theodisiou, Athena Vakali, Anastasis Kounoudes	2019	According to this study, the Twitter application is stated to be safer than Instagram. This can be seen in terms of threats to security and privacy on the Twitter application less than Instagram.
13	An Effective Approach to Mobile Device Management: Security and Privacy Issues Associated with Mobile Applications	Darren Hayes, Francesco Cappa, Nhien An Le-Khac	2020	This study found Instagram has more weaknesses compared to Twitter. Therefore twitter is superior to Instagram.
14	Facebook, Twitter, and Instagram: The Privacy Challenges	Amira Farah Abdul Rashid, Zarul Fitri Zaaba	2020	Based on this article, Instagram and Twitter have similarities in terms of privacy and data security.
15	Influencing Photo Sharing Decisions on Social Media:A Case of Paradoxial Findings	Mary Jean Amon, Rakibul Hasan, Kurt Hugenberg, Bennettl. Bertenthal, and Apu Kapadia.	2020	Instagram and Twitter both have privacy settings to control who can see content from users.
16	Information Privacy Concerns Among Instagram Users: The Case of Indonesian College Students	Eko Wahyu Tyas Darmaningrat, Hanim Maria Astuti, and Fadhila Alfi	2020	Instagram gives you the option to approve or reject new followers on private accounts. Users can also control comments and tags on their photos, and have the option to report or block other unwanted users.
17	The Fragmented Self: Having Multiple Accounts in Instagram Usage Practice among Indonesian Youth	Mashita Phitaloka Fandia Purwaningtyas and Desti Ayu Alicya	2020	Users of both platforms can have more than one account for increased security and privacy. Users can manage and restrict access to their personal information.
18	Enterprise Credential Spear-phishing attack detection	Yuosuf Al-Hamar, Hoshang Kolivand, Mostafa Tajdini, Tanzila Saba, and Varatharajan Ramachandran	2021	There are differences in the effectiveness of different email security systems between Instagram and Twitter in detecting phishing attacks.
19	Online Profiling of Social Network Platforms: Twitter vs. Twitter Instagram	Veruska Ayora, Flavio Horita, and Carlos Kamienski	2021	On Instagram, data permissions are tightened platform policies are updated, and regularly evaluate app access to user permissions. While on Twitter, the algorithm on the platform continues to be improved, transparency and accountability.
20	Towards the creation of a profile of the information privacy aware user through a systematic literature review of information privacy awareness	Aikaterini Soumelidou and Aggeliki Tshohou	2021	Instagram allows users to manage their data usage with third-party apps. Twitter provides control over the use of data for advertising and allows users to opt out of viewing sensitive content.
21	My Social Network: Group Differences in Frequently of Use, Active Use, and Interactive Use on Facebook, Instagram, and Twitter.	Tal Laor	2022	Twitter application is safer than the Instagram application. This is shown by the composition of Twitter users presenting less personal data. Unlike Instagram, which is often used to post something about users.

22	Study of Security and Privacy Measures on Twitter and Instagram	Fatin Izzati bint Fammy Rikzan and Mohd Khair Udin Kasiran	2023	The study's finding is that Instagram and Twitter both offer settings to protect their accounts from unwanted access. Privacy allows users to control private or public visibility.
23	The mediating role of perceived risks and benefits when self-disclosing: A study of social media trust and FoMO	Karl van der Schyff and Stephen Flowerday	2023	Instagram, which is owned by Meta, has privacy features such as personal account settings and the ability to control who can see users' posts and stories. However, Instagram does not have an audience selector feature.
24	Securing online accounts and assets: An examination of personal investments and protection motivation	Obi Ogbanufe	2023	Instagram and Twitter both offer security features, such as two-factor authentication (2FA) or multi-factor authentication (MFA), which can prevent 99.9% of account hacks.
25	Privacy Protection Strategies on Social Media.	Muhammad Zulfahmi, Anthony Elsandi, Aldizar Apriliansyah	2023	In this study, Instagram and Twitter tend to be the same.

Various studies have shown that Instagram and Twitter have different data security and privacy design systems. However, between the two, pay attention to maintaining security and user privacy through the features in the application. In addition, there are also differences in the effectiveness of the security system between the two social media platforms.

Discussion

Instagram and Twitter have the same power to deliver content to millions of people quickly. However, it does not rule out the possibility of a debate between Instagram and Twitter regarding the number of users, convenience, etc. Most of these debates do arise because they both have the same audience. This is proven by the fact that Instagram and Twitter are quite dominated by the younger generation. This group is indeed a market for social media platforms. The number of Instagram and Twitter users also illustrates the amount of data stored by the database of systems that work in it. If it looks back, the way Instagram and Twitter applications work is not too much different. However, note that each system's data security and privacy protection levels are always different.

Before starting activities on social media, what the user does is log in to the system. The log-in system is the first gateway that protects users from unauthorized access and is an important aspect of the online security infrastructure. Instagram has a login system allows users to enter a username and password, even through a Facebook account. Twitter must provide a username/email with the appropriate password. Research conducted by Obi Ogbanufe (2023) shows that Instagram and Twitter have implemented additional security measures in the login process, such as two-factor authentication. However, it is necessary to be aware of existing threats, in line with a study by Al-Hamar (2021), which found that thieves created fake Instagram social media phishing pages to get victims' usernames and passwords. Users are asked to enter their login information, which is then stolen and sold. Researchers also consider the findings of Ayora et al. (2021) that security algorithms are constantly tightened and updated to evaluate application access to user permissions.

One useful security aspect of controlling their interactions and keeping unwanted users safe online is through blocking. According to Rikzan & Kasiran (2023), Instagram and Twitter both offer settings to block other annoying or dangerous users. Soumelidou & Tsohou (2021) added that Instagram provides reporting tools for users to report suspicious activity or content that violates community guidelines. This shows that Instagram allows users to block individuals and provides a means to report inappropriate behavior. In line with a study by Rashid & Zaaba (2020), a blocking system is beneficial because it allows users to reduce account hacking.

To ensure additional protection, a security measure that can be taken by users is to enable two-factor authentication, namely by asking users to verify their identity using a verification code via text message or authentication application. So, users need a verification code to access their account if their password has been leaked. Research by Shevchuk & Pastukh (2018) showed that Twitter has developed its ever-evolving detection methods to address security concerns. Instagram leverages the "Facebook Immune System" as part of the ecosystem. This shows that the two platforms have different approaches to implementing and improving their security systems, including 2FA. Gan & Jenkins (2015) also emphasize the importance of users actively managing their security settings on Twitter, which may include enabling 2FA. However, Ogbanufe (2023) mentions a person's indifference to account authentication due to a lack of motivation associated with how much investment they provide in the form of time, effort, relationships, and social interactions. About 71% of online accounts are protected with one-factor passwords, often ineffectively reused across multiple online accounts or not changed in five years or more (Ogbanufe, 2023).

An important aspect of privacy settings that allow users to decide whether they want their profile to be visible to the public or only by certain circles is part of the profile's visibility. Rikzan & Kasiran (2023), Instagram and Twitter offer settings to protect accounts from unwanted access, allowing users to control private or public visibility. However, Gritzalis et al. (2014) point out that although both platforms offer privacy settings, users are often unaware that shared information may pose a threat. Choi & Sung (2018) believe that profile visibility, disclosure of personal information, self-disclosure, and self-expression are major issues in social media privacy. Social media user behavior is influenced by regions and cultures where many use pseudonyms (Cengiz et al., 2022). On the other hand, Purwaningtyas & Alicya (2020) stated that most people feel worried about the persona built on the internet through the use of main and second accounts. In line with Bhatnagar & Pry's (2020) research, most students surveyed use security features and set their social media accounts to private.

Post control is an important aspect of the social media experience that allows users to determine how and with whom their content is shared. The study by Aman et al. (2020) stated that participants were asked to consider the privacy of photo subjects. The results show that people don't have strong privacy preferences and prefer to share photos. Instagram allows control of posts shared with users. Instagram with private accounts can approve or reject new followers, giving them more control over who can see their content and controlling comments and tags on photos. Users can choose who can see or interact with them like the "Close Friends" feature. Twitter also allows users to set their profiles to only approved followers. However, Twitter does not have an audience selector feature

Research that has been conducted shows that both of these platforms have privacy features and settings designed to protect their users. Researchers have formulated and considered several aspects of data security and user privacy for comparing social media platforms Instagram and Twitter. These considerations refer to the article of Rashid & Zaaba (2020). So, a comparison is produced as follows.

Table 2. Comparison of data security and user privacy between Instagram and Twitter

Security and Privacy Aspects	Instagram	Twitter
Log-In System	Use a username and password. Log-in is also supported with the Facebook app.	Verify your email to create an account (log-in credentials).
Blocking System	The blocked user can't find the blocker account, so there's no interaction.	Blocked users will know if their account is blocked because Twitter views will still be visible but unable to interact.
Two-Factor Authentication	Option to enter an additional layer of security through an additional verification code.	To increase security, users can turn on two-step verification.
Profile Visibility	There is a "Public" or "Private" option.	There are "Public" or "Protected" options.

Post Control	Set the account as public or private, choosing to approve the tag beforehand.	Set tweets as public or protected and limit who can see and respond.

The comparison table compiled in this study shows the differences and similarities between the data security and user privacy features offered by Instagram and Twitter. By understanding and comparing these five aspects, researchers seek to provide deeper insights into the level of security offered by Instagram and Twitter.

Based on the findings and analysis that has been done, it is shown that both platforms, Instagram and Twitter, are equipped with data security and privacy settings designed to protect users. The analysis that has been done answers research questions that show that Instagram users tend to be superior to Twitter regarding data security and privacy. This statement is supported by several studies, including research by Giridhar et al. (2017); (Shane-Simpson et al. (2018); and Paramarta et al. (2018). Despite this, Instagram remains vulnerable to data security and user privacy threats.

The difference in the effectiveness of security and privacy systems means exploring applicable prevention strategies further is important. Therefore, researchers recommend some prevention of these security and privacy threats that can help users protect their personal information in the digital world, such as user education, enabling two-factor authentication, tighter privacy settings, routine changing passwords, and account activity supervision. By implementing the aforementioned strategies, users can reduce the risk of data leakage and misuse of their personal information on social media platforms such as Instagram and Twitter. Such implementations protect their data and privacy and contribute to a safer and more trusted social media environment for all users.

4. CONCLUSION

A comparative analysis of 25 journal articles on data security and privacy on two popular social media platforms, Instagram and Twitter, found that each platform has advantages and weaknesses regarding data security and user privacy. In addition, both platforms have security systems designed to protect their users despite differences in the effectiveness of those systems. Through a comprehensive analysis of the literature, the study found answers to the research question that Instagram has advantages in data security and privacy compared to Twitter, which is supported by several related studies. Despite this, users should still be wary of threats such as phishing. Therefore, users are advised to develop effective strategies that include user education, activation of two-factor authentication, stricter privacy settings, regular password changes, and monitoring of account activity to prevent data security and privacy threats. The limitations of this study mainly lie in data collection methods that rely on electronic databases that may not include all relevant reference sources, which may lead to bias in data discovery. In addition, eliminating information the author carries out to determine the quality and relevance of scientific articles may also affect the study's final results. The study also uses a qualitative approach through literature studies, which, while enabling a deeper understanding of social media data security and privacy issues, do not provide quantitative data that can be used to measure or compare data security and privacy levels directly. Thus, it is hoped that future research can provide more relevant and up-to-date recommendations, which will greatly benefit users in maintaining their data security and privacy in an ever-evolving digital world.

REFERENCES

Abhinav, S., Sonalika, K., Charu, C., Yadav, C. P., & Lokesh, K. (2023). Meta-analysis on Plasmodium falciparum sulfadoxine-pyrimethamine resistance-conferring mutations in India identifies hot spots for genetic surveillance. *International Journal of Antimicrobial Agents*. *63*(3). https://doi.org/10.1016/j.ijantimicag.2023.107071

Al-Hamar, Y., Kolivand, H., Tajdini, M., Saba, T., & Ramachandran, V. (2021). Enterprise Credential Spear-phishing attack detection. Computers and Electrical Engineering, 94 (September 2021). https://doi.org/10.1016/j.compeleceng.2021.107363

Aman, K. D. (2023). Study of Security and Privacy Measures on Twitter and Instagram. 6(3), 49–55.

Amon, M. J., Hasan, R., Hugenberg, K., Bertenthal, B. I., & Kapadia, A. (2020). Influencing photo sharing decisions on social media: A case of paradoxical findings. Proceedings - IEEE Symposium on Security and Privacy, 2020-May, 1350–1366. https://doi.org/10.1109/SP40000.2020.00006

Anwer, M. A., Zarro, R. D., & Farraj, K. H. (2017). Security Issues in Social Media: Challenges and Solutions. 6566(April), 408–420. https://doi.org/10.25212/lfu.qzj.2.2.41

Arendt, H. (1958). The Human Condition 2nd ed. Chicago: University of Chicago Press.

Ayora, V., Horita, F., & Kamienski, C. (2021). Profiling online social network platforms: Twitter vs. Instagram. Proceedings of the Annual Hawaii International Conference on System Sciences, 2020-Janua, 2792–2801. https://doi.org/10.24251/hicss.2021.341

Bhatnagar, N. (2020). Student attitudes, awareness, and perceptions of personal privacy and cybersecurity in the use of social media : An initial study. 18(February), 48–58.

Boyd, D., & Ellison, N. (2007). Social Network Sites: Definition, History, and Scholarship. Journal of Computer-Mediated Communication, 13(1), 210–230. https://doi.org/10.1111/j.10836101.2007.00393.x

Cengiz, A. B., Kalem, G., & Boluk, P. S. (2022). The Effect of Social Media User Behaviors on Security and Privacy Threats. IEEE Access, 10, 57674–57684. https://doi.org/10.1109/ACCESS.2022.3177652

Choi, T. R., & Sung, Y. (2018). Instagram versus Snapchat: Self-expression and privacy concern on social media. Telematics and Informatics, 35(8), 2289–2298. https://doi.org/10.1016/j.tele.2018.09.009

Darmaningrat, E. W. T., Astuti, H. M., & Alfi, F. (2020). Information Privacy Concerns Among Instagram Users: The Case of Indonesian College Students. Journal of Information Systems Engineering and Business Intelligence, 6(2), 159. https://doi.org/10.20473/jisebi.6.2.159-168

Dashora, D., Ashok, P., & Jetawat, K. (2017). An Assessment Cram on Security Issue of Fake Identity Behavior in Social Media. 34–37.

Gan, D., & Jenkins, L. (2015). Social Networking Privacy—Who's Stalking You? Future Internet, 7(4), 67–93. https://doi.org/10.3390/fi7010067

Gangarde, R., Sharma, A., & Pawar, A. (2019). Bibliometric survey of privacy of social media network data publishing. Library Philosophy and Practice, 2019(July 2023), 1–21.

Giridhar, P., Wang, S. , Abdelzaher, T., Amin, A., and Kaplan, L., (2017). "Social Fusion: Integrating Twitter and Instagram for Event Monitoring," 2017 IEEE International Conference on Autonomic Computing (ICAC), Columbus, OH, USA, pp. 1-10, doi: 10.1109/ICAC.2017.46

Gritzalis, D., Kandias, M., Stavrou, V., & Mitrou, L. (2014). History of Information: The case of Privacy and Security in Social Media. Proceedings of the History of Information Conference, 283–310. http://www.cis.aueb.gr/Publications/INFOHIST-2014 Legal Publications.pdf

Hafidz, I., Kautsar, A. R., Valianta, T., & Rakhmawati, N. A. (2017). Teenstagram TimeFrame: A Visualization for Instagram Time Dataset from Teen Users (Case Study in Surabaya, Indonesia). Procedia Computer Science, 124, 100–107. https://doi.org/10.1016/j.procs.2017.12.135

Hayes, D., Cappa, F., Le-Khac, N. A., (2020). An effective approach to mobile device management: Security and privacy issues associated with mobile applications, Digital Business, *1*(1), https://doi.org/10.1016/j.digbus.2020.100001

Kaur, R., Singh, S., & Kumar, H. (2018). Rise of spam and compromised accounts in online social networks: A state-of-the-art review of different combating approaches. Journal of Network and Computer Applications, 112(February), 53–88. https://doi.org/10.1016/j.jnca.2018.03.015

Kharbat, F. F., & Abu Daabes, A. S. (2019). Privacy paradoxes in the middle east: A content analysis from instagram. Proceedings - 2019 International Arab Conference on Information Technology, ACIT 2019, 287–288. https://doi.org/10.1109/ACIT47987.2019.8991070

Lim, J. S., Heinrichs, J. H., & Lim, K. S. (2017). Gender and hedonic usage motive differences in social media site usage behavior. Journal of Global Marketing, 30(3), 161-173.

Mistry, V. (2011). Critical care training: using Twitter as a teaching tool. British Journal of Nursing, 20(20), 1292-1296.

Moustaka, V., Theodosiou, Z., Vakali, A., Kounoudes, A., Anthopoulos, L. G., (2019). Enhancing social networking in smart cities: Privacy and security borderlines, Technological Forecasting and Social Change, Volume 142, Pages 285-300, ISSN 0040-1625, https://doi.org/10.1016/j.techfore.2018.10.026.

Oehri, C., & Teufel, S. (2012). Social media security culture - The Human Dimension in Social Media Management. In Information Security for South Africa, 4(1), 1–5.

Ogbanufe, O. (2023). Securing online accounts and assets: An examination of personal investments and protection motivation. International Journal of Information Management, 68(July 2022), 102590. https://doi.org/10.1016/j.ijinfomgt.2022.102590

Okditazeini, V., & Irwansyah. (2018). Threat on Privacy and Data Mining in Digital Era: a Meta-Synthesis Analysis on Social Networking Sites (Sns). Jurnal Studi Komunikasi Dan Media, 22(2), 109–122. https://www.journals.sagepub.com on Information Systems, ICIS 2012, 3(Ftc 2009), pp. 2278–2293.

Paramarta, V., Jihad, M. Dharma, A., Hapsari, I. C., Sandhyaduhita, P. I., Hidayanto, A. N., (2018). Impact of User Awareness, Trust, and Privacy Concerns on Sharing Personal Information on Social Media: Facebook, Twitter, and Instagram. *2018 International Conference on Advanced Computer Science and Information Systems (ICACSIS)*. https://doi.org/10.1109/ICACSIS.2018.8618220

Pawestri, F. D., & Jumino, J. (2021). Analisis Hubungan Information Privacy Concern dan Perilaku Perlindungan Privasi Pengguna Twitter di Indonesia. Anuva: Jurnal Kajian Budaya, Perpustakaan, dan Informasi, 5(2), 221-236.

Purwaningtyas, M. P. F., & Alicya, D. A. (2020). The Fragmented Self: Having Multiple Accounts in Instagram Usage Practice among Indonesian Youth. Jurnal Media Dan Komunikasi Indonesia, 1(2), 171. https://doi.org/10.22146/jmki.58459

Rashid, A. F. A. and Zaaba, Z. F., (2020). "Facebook, Twitter, and Instagram: The Privacy Challenges," 2020 International Conference on Promising Electronic Technologies (ICPET), Jerusalem, Palestine, pp. 122-127, doi: 10.1109/ICPET51420.2020.00032.

Rejeb, A., Rejeb, K., Abdollahi, A., & Treiblmaier, H. (2022). The big picture on Instagram research: Insights from a bibliometric analysis. Telematics and Informatics, 73(December 2021), 1–28. https://doi.org/10.1016/j.tele.2022.101876

Rikzan, F. I. F., & Kasiran, M. K. (2023). Study of Security and Privacy Measures on Twitter and Instagram. *Borneo International Journal. 6*(3). https://majmuah.com/journal/index.php/bij/article/view/531

Shane-Simpson, C., Manago, A., Gaggi, N., & Gillespie-Lynch, K. (2018). Why do college students prefer Facebook, Twitter, or Instagram? Site affordances, tensions between privacy and self-expression, and implications for social capital. Computers in Human Behavior, 86, 276–288. https://doi.org/10.1016/j.chb.2018.04.041

Shevchuk, R., & Pastukh, Y. (2019). Improve the Security of Social Media Accounts. IEEE, 6–9.

Soumelidou, A., & Tsohou, A. (2020). Effects of privacy policy visualization on users' information privacy awareness level: The case of Instagram. Information Technology and People, *33*(2). https://doi.org/10.1108/ITP-08-2017-0241

Soumelidou, A., & Tsohou, A. (2021). Towards the creation of a profile of the information privacy aware user through a systematic literature review of information privacy awareness. Telematics and Informatics, 61(February), 101592. https://doi.org/10.1016/j.tele.2021.101592

Statista. (2020). "Leading countries based on number of Twitter users as of October 2020". https://www.statista.com/statistics/242606/number-of-active-twitter-users-in-selected-countries/.

Tal Laor (2022). My social network: Group differences in frequency of use, active use, and interactive use on Facebook, Instagram and Twitter, Technology in Society. 68. https://doi.org/10.1016/j.techsoc.2022.101922.

van der Schyff, K., & Flowerday, S. (2023). The mediating role of perceived risks and benefits when self-disclosing: A study of social media trust and FoMO. Computers and Security, 126. https://doi.org/10.1016/j.cose.2022.103071

Xu, H. et al. (2012), 'Measuring mobile users' concerns for information privacy', International Conference

Zhang, W., & Sun, H. M. (2017). Instagram spam detection. Proceedings of IEEE Pacific Rim International Symposium on Dependable Computing, PRDC, 227–228. https://doi.org/10.1109/PRDC.2017.43

Zulfahmi, M., Elsandi, A., Apriliansyah, A., Anggreainy, M. S., Iskandar, K., Karim, S. (2023). Privacy protection strategies on social media, Procedia Computer Science. 216. https://doi.org/10.1016/j.procs.2022.12.159.