ISSN 2723-6471

Meta-Analysis of Social Networking Sites for the Purpose of Preventing Privacy Threats in the Digital Age

Teresa Alvarez [1,*], Hsieh-Chih Chen [2]

[1] University of Valladolid, Spain
[2] National Sun Yat-sen University/Kao Yuan University, Taiwan
tere@autom.uva.es [1,*]; t90105@cc.kyu.edu.tw [2]
* corresponding author

(Received July 4, 2021 Revised August 10, 2021 Accepted August 28, 2021, Available online September 29, 2021)

Abstract

This article will discuss the challenges to privacy and data mining in social networking sites (Social Networking Sites). The author begins by defining privacy and data mining in today's big data sector before doing a meta-synthesis analysis. Numerous references and literature reviews were undertaken in order to compile material pertinent to the topic of privacy risks and data mining on social networking sites. According to the researchers' conceptualization, privacy concerns and data mining on SNS can be classified into three categories: multimedia content threats, traditional threats, and social threats. Each category is subdivided into multiple threat types. The author notes that in addition to utilizing the privacy measures offered by the SNS site, users must develop an early understanding of the difference between information and secrets. Users must use caution when deciding what content to share on social media platforms and what not to share.

Keywords: SNS, Privacy Threats, Social Networking

1. Introduction

Online social networking (Social Networking Sites/SNS) is an inseparable part of the social life of today's society. Of course, this is inseparable from technological advances that have invaded the patterns and patterns of community interaction. Coupled with new technology that is increasingly aggressively developing innovations so that people indirectly have to follow suit. SNS is a means to overcome most problems in various fields, be it communication, bureaucracy, entertainment, education, and others. With its fast, easy, and low cost innate nature, social media is an alternative for keeping in touch with other people.

This SNS has become popular because it facilitates users to stay connected (log in) continuously so that these users can still receive messages from colleagues and relatives every day. Users can connect with other virtual communities, be it with family, friends, coworkers, and even with people they don't know at all. According to Henson et al., in recent decades SNS has evolved from an entertaining new world into a multibillion dollar global industry, with users from all walks of life. Thus, this gave rise to a new industry in SNS.

The use of SNS encourages a person to disclose personal information (eg age, sexual or political orientation, date of birth, purchase of an item, etc.). Of course, the disclosure of personal information is full of risks. As research conducted by Clemens et al. [1], it is suspected that disclosure of this information can result in identity theft or sanctions at school or work for raising a sensitive issue. In his research, Henson et. al showed that around 42% of student SNS users experienced some form of privacy threat during their lifetime, this is an important issue that requires further attention.

Social Networking Sites (SNS) is a type of web service to build a virtual network among people who have similar interests, backgrounds and activities. SNS can be very beneficial to its users as it removes economic and geographic boundaries, and can also be useful in achieving goals related to job search, entertainment and education. However, Rathore et al. [2] identified that the popularity of SNS also creates a high risk for its users. When some personal data is shared on SNS it makes users tempting targets for attacks, such as spam, malware, socialbots and identity theft. Even attackers can also find other significant data, such as bank account information, which is then used for crimes such as fraud, then personal identity and location.

This paper will elaborate on how the threats to privacy and data mining in SNS are. By first explaining the concept of privacy and data mining itself in today's big data industry, the author offers a conceptual explanation. Various references and literature studies were conducted to find data relevant to the issue of privacy threats and data mining on SNS. Based on the background that has been described, the authors limit the problem to the following:

- What are the threats to privacy and data mining in online social networks (SNS)?
- How are threats to privacy and data mining conceptualized in the digital industry?

2. Literature Review

3.1. Privacy

Sissela Bok defines privacy as a realm where personal concerns and freedoms are not compromised. From a legal point of view, the courts have ruled that the right to privacy is a fundamental aspect of Western culture. In the United States, Samuel Warren and Louis D. Brandeis first conceptualized privacy as a legal formulation in their 1899 essay: 'The Right to Privacy'. Thus, privacy law focuses on 'the prohibition against profound disturbances of human dignity by those with economic or governmental power'.

Wolak et al. [3] examined the relationship between online interactions/activities and the initiation of harm to one's privacy on the Internet. They concluded that posting personal information or using SNS is not in itself risky behavior, but interacting with strangers and having strangers on friends lists makes teens vulnerable to privacy threats on SNS. It appears with whom users share sensitive information is more important in preventing online privacy threats than setting one's profile to private access, both among youth and students.

The results of research conducted by Milham and Atkin [4] confirm and expand the historical exploration of the relationship between privacy attitudes and personal identity disclosure behavior, especially among users who place greater attention on their personal information and feel protective of it. Milham and Atkin's findings are in line with previous research conducted by Child et al. [5] regarding the disclosure of private information to the public. The results of Child et al.'s study confirm that users who pay greater attention to privacy issues are less likely to become victims of abuse on SNS. Today's highly interactive website designs encourage the unconscious oversharing of personal information, one of which SNS users are concerned about.

Privacy is a culture-specific phenomenon. As the SNS platform becomes global, the question of privacy practices in a cross-cultural context becomes increasingly important. A study from Liang et al. [6] examined cultural variations of profile settings in privacy and self-disclosure through geolocation facilities on Twitter. Liang et al. randomly selected 3.3 million Twitter accounts from more than 100 demographic groups. The results of his research reveal that cultural and community differences are quite large in influencing the behavior of SNS users in using privacy settings on their accounts. Privacy settings in collective societies are more effective in promoting self-disclosure, and appear to be less important for users in individualistic societies. Internet penetration is also a significant factor in predicting both the adoption of privacy settings and self-disclosure geolocation.

With the diffusion of Internet technology, online privacy has become a major problem facing all Internet users. Accidental leakage of personal information can lead to a series of negative consequences such as account abuse, unsolicited email or phone calls, or even financial loss. Many SNS users expressed serious concern about the leakage of personal information online. However, according to Rainie and Madden [7], only 30% of all US adults have taken these steps to protect their privacy online, such as changing their privacy settings at SNS.

The difference in attitude to changing privacy rules for some users is due to the way in which SNS is used today; that is, cyberspace is dominated by SNS platforms. According to Boyd [8], privacy practices on SNS platforms are often paradoxical. On the one hand, Internet users are often motivated to disclose personal information to present a unique identity that distinguishes themselves from others and accumulates social capital in SNS. On the other hand, SNS companies retain a large amount of personal information collected from their users, and such information can be easily misused.

To help solve this dilemma, almost all popular SNS platforms allow users to customize their privacy settings. Users can create deterministic rules that define which pieces of content will be shared, and with whom that content can be accessed. According to Stutzman et al. [9], when controlling their privacy, individuals tend to disclose more information. Many studies have been conducted to understand privacy protection behavior on social media platforms.

3.2. Data Mining

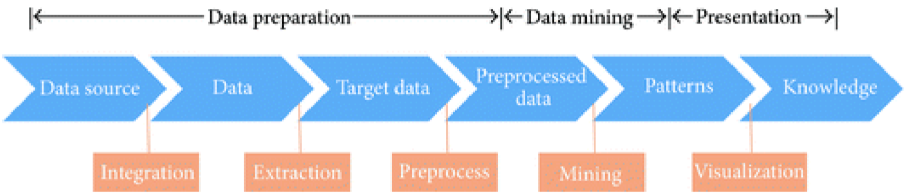

Figure. 1. Overview Data Mining

According to Chen et al., data mining is the process of finding interesting knowledge from large amounts of data stored either in databases, data warehouses, or other information repositories. Based on the definition of data mining and the definition of data mining functions, a common data mining process includes the following steps:

- Data preparation: preparing data for mining. It includes 3 steps of integrating data in multiple data sources and cleaning noise from data. extract some parts of the data into the data mining system, pre-process the data to facilitate data mining
- Data mining: applying algorithms to data to find patterns and evaluate patterns of knowledge found
- Data presentation: visualize data and represent mined knowledge to users

Kennedy et al. [10] identify as global use of SNS grows, so does data mining in SNS. SNS data can be understood as what is said and shared on SNS, who says and shares it, where they are, who they are connected to, how influential and active they are and what their previous activity patterns are. Data mining encompasses a wide range of activities undertaken to analyze, organize, classify and understand the data, from calculating content likes and shares to measuring reach, sentiment and key influencers, using techniques such as social network analysis, problem network analysis and natural language processing, and others.

Kennedy et al. [10] also confirm that the rise in SNS data mining has been driven by a number of factors: increased availability of data on users and their online behavior, as more social activities take place online; reduced costs of data collection, data storage and processing; and the expansion of the SNS platform from which much of this data is drawn. Mined SNS data is often combined with data from other sources, such as Edward Snowden's disclosures about the data mining operations of the National Security Agency in the United States and the Government Communications Headquarters in the United Kingdom. In his research, Hill [] also finds cases of data mining, for example, in targeted advertising, such as the widespread case of a young woman whose father became aware that she was pregnant when an online department store targeted advertisements for pregnancy-related products to her as results from tracking his online behavior. This everyday occurrence deserves to be studied as a form of data mining that must be paid more attention to.

The results of the research by Kennedy et al. [11] show that many SNS users feel injustice over their personal data taken from them. According to him, the discomfort of some informants with what the SNS platform does with their information and data shows that there is a difference between platform practices and users' normative expectations. Participants' consideration of how to ensure greater transparency in relation to data mining practices, in turn, seemed to indicate interest among SNS users in the possibility of a more equitable SNS world.

3.3. Big Data

The term “big data” has become one of the most talked about things in recent decades. According to the Wikibon site, the estimated market value of big data was US$50.1 billion in 2015. The rapid expansion of the big data market has had a particular effect on the emergence of new publication models and their use in different fields such as human digital and election prediction in a leader election campaign. The application of big data problems that have penetrated into various commercial areas has resulted in major changes in the industry with a direct impact on human life, such as insurance, health care, or banking, and others.

Big data is a broad term used for a data set that has a size (e.g., dimensions, volume, and speed) and complexity (e.g. diversity, variability) that exceeds the capabilities of tools used traditionally to capture, process and analyze data over long time frames. tolerable. In the social sciences, “big data” refers to data sets that are too large for humans to code for a representative sample of the entire dataset. Research conducted by Kitchin and McArdie [12], identified 7 (seven) characteristics of big data:

- Flexibility (overall data system)
- Networked fine (has a small resolution) and unique (between one data and another data is different, especially marked with a URL)
- Relational (can be generalized and allows to be merged from different datasets)
- Extensibility (can add/change new fields easily) and scalability (can expand in size quickly)
- Truth (data can be messy, crowd and contain uncertainty and error)
- Value (lots of insights can be extracted and data transferred)
- Variability (data whose meaning can constantly change in relation to the context in which they are generated)

Frith [13] elaborates on the spread of big data in seeing the growth of smart cities. The term smart city refers to the use of digital technology to generate data that can improve city efficiency, citizens' livelihoods, and improve citizen safety. In this article Frith uses the phrase smart city to refer to data-driven urban projects in cities. Examples of the application of big data in smart cities are the use of sophisticated transportation modes, technology for detecting and mitigating disasters, the use of electronic money, and others.

3.4. Conceptualization of Privacy and Data Mining Threats

Threats to privacy and data mining were comprehensively conceptualized by Shailendra Rathore, Pradip Kumar Sharma, Vincenzo Loia, Yong-Sik Jeong, and Jong Hyung Park in 2017 in their article Social Network Security: Challenges, Threats, and Solutions. According to Rathore et al., in relation to privacy and data mining threats, there are several categories of threats, including:

1) Threats to Multimedia Content
   The types of threats that occur in this category are:
   - Multimedia content exposure
   - Co-ownership
   - Content manipulation

- Steganography
- Metadata
- Shared link
- Data transparency
- Tags

2) Traditional Threat
    - Phishing, which is the act of obtaining personal information such as User ID, Password, and other sensitive data by impersonating an authorized person or organization via an email.
    - Malware (Malicious Software), which is a program designed with the aim of causing damage by infiltrating computer systems. Malware includes viruses, worms, trojan horses, most rootkits, spyware, dishonest adware, and other software that is harmful and unwanted by PC users.
    - Sybil attacks and fake profiles, namely activities using fake accounts to threaten the security of computer users.
    - Spamming, which is the activity of sending fake emails by using an email server that has an "smtp open relay" or sending information or advertisements for a product that is not in place and this is very disturbing for those who are sent.
    - Deanonymization attack, which is a strategy in data mining where unknown (anonymous) data is referred to other data sources to identify anonymous data sources.
    - Profile cloning attack, which is a term used for forging a profile/identity to outwit someone.
3) Social Threat
    - Cyber-bullying, namely all forms of violence experienced by children or adolescents and carried out by friends their age through the internet.
    - Cyber-stalking, which is a crime committed to annoy or harass someone by using a computer, for example using email, and is done repeatedly.

3. Research Method

This paper is a conceptual paper that adapts the meta-synthesis guidelines from Francis and Baldesari with a qualitative meta-aggregation approach. A qualitative approach in meta-synthesis is used to synthesize (summarize) the results of research that are descriptive qualitative. This method of synthesizing (summarizing) the results of qualitative research is called "meta-synthesis". By definition, meta-synthesis is a technique of integrating data to obtain new theories or concepts or a deeper and more comprehensive level of understanding.

In conducting meta-synthesis (synthesis of qualitative data) there are 2 (two) approaches, namely meta-aggregation (meta-aggregation) and meta-ethnography (meta-ethnography). In meta-aggregation, synthesis aims to answer research questions (review questions) by summarizing various research results (summarizing). Meanwhile, meta-ethnography, synthesis aims to develop a new theory in order to complement the existing theory.

In meta-aggregation, research topics are elaborated into certain themes to produce a conceptual framework. Then, within certain themes, relevant research articles are searched and compared and summarized between one another. In the meta-aggregation approach, the results of the synthesis are “aggregates” of various research results according to the relevant themes. Francis and Baldesari identify the steps in conducting meta-synthesis:

3.1. Formulating the review question

The focus of this study is to find out how privacy and data mining threats are on Social Networking Sites (SNS). For this reason, several questions are designed to be answered from the results of this literature review.

H1: In what publication forums are discussions on privacy and data mining published?

H2: What are the problems/issues found in the existing research?

H3: How does each concept contribute to the integration of SNS?

3.2. Conducting a systematic literature search

In this literature review, the data sources that will be used are papers available on the ScienceDirect website page. The more data sources used, the greater the possibility to find suitable literature. The strategy in conducting a search is built through determining keywords and synonyms from the focus of the study.

3.3. Screening and selecting appropriate research articles

The application of this search is likely to produce a large number of papers. Therefore, further identification is needed to obtain papers that can be used as primary studies. Identification can be done by applying inclusion and exclusion criteria. The application of these inclusion and exclusion criteria will ensure that the paper used is a paper that truly fits the context of the study.

1) Inclusion Criteria
    - Papers that explain the concepts, benefits, techniques, methods, strategies, and everything in the application of privacy and data mining on SNS simultaneously
    - Papers presented in English.
2) Exclusion Criteria
    - Papers that only focus on discussing privacy on SNS only
    - Papers that only focus on discussing data mining on SNS only
    - Papers that focus on discussing privacy in SNS with concept disciplines other than data mining
    - Papers that focus on discussing data mining in SNS with concept disciplines other than privacy

3.4. Analyzing and synthesizing qualitative findings

The procedure for selecting papers is done by speed reading all candidates for primary studies. Speed reading is reading the abstract part of the available paper. Furthermore, based on the inclusion and exclusion criteria, it can be determined whether the paper can be used as a primary study.

3.5. Maintaining quality control

Based on the review plan that has been prepared, the next step is to execute the plan. The search execution on the website page that was used as the data source resulted in 151 papers which were candidates for primary studies.

4. Result and Discussion

Various studies on big data analysis identify a number of cases that are potentially dangerous for users. According to research conducted by Dixon and Gellman [14], the availability of large consumer databases has resulted in a thriving industry of unregulated consumer scores. Pasquale [15] identified that this user data deployment logic is based on algorithmic logic that can predict any incoming data from an increasingly massive cross-context database, sorting individuals into segments in areas as diverse as employment, rental or retail. Therefore, beyond the technical aspects of big data processing and its practical applications, according to Andrejevic [16], big data seems to produce a new social organization of knowledge that normalizes the climate of loss of privacy while reproducing or even accentuating existing inequalities.

Gavinson [17] introduced the term individual autonomy, that privacy should protect the individual's power over how to determine one's own destiny and, at the very least, the individual's capacity for self-definition. In a data collection environment, the discussion of privacy is complicated by the alleged difficulty of defining privacy violations in individuals. According to Solove [18], efforts have been made in recent years to update privacy protections for alleged digital data collection, while maintaining a literacy strategy that assumes privacy-conscious users.

With the current development of SNS, issues related to how to maintain the privacy and security of users are also starting to emerge, especially when users upload multimedia content such as photos, videos and audio. Henson et al. also identified that with today's large number of online users also growing online threats on SNS sites. This can be overcome by individuals by creating 'self-defense' by using the privacy features of existing SNSs. Because in the end, the first layer of protection must be done by the user himself.

According to Harris [19], network security is censorship of networks/content that is prohibited online, which is processed in an organized manner and implemented through vertical control. SNS has become a mainstream cultural phenomenon for millions of internet users. Combining user-generated profiles with communication mechanisms that allow users to become in touch on a pseudo-permanent basis, SNS leverages users' real-world social relationships and blends more of users' online and offline lives. In 2017, Facebook had 1.94 billion monthly active users and it was the third most visited site on the Internet. Twitter, the social microblogging platform, claims more than 313 million monthly active users, who post Tweets in more than 40 languages.

Since users on SNSs typically connect with friends, family, and acquaintances, the general perception that has emerged is that SNSs provide a more secure, private, and trusted Internet-mediated environment for online interactions. In reality, however, SNS has raised the stakes for privacy protection due to the availability of an unexpectedly large amount of personal user data, whether published or not. More importantly, SNS exposes information from a variety of social areas for example, personal information on Facebook and professional activity on LinkedIn which is aggregated and leads to more detailed profiles.

This unsolicited disclosure of user information causes SNS to have dire consequences. The news media covered some of these, such as the case of a teacher being sued for posting a shotgun photo, or an employee being fired for commenting on his salary compared to his boss (both are cases on Facebook). Moreover, SNSs themselves, either intentionally (e.g. the Facebook Beacon controversy) or inadvertently (e.g., publishing anonymous social data used to de-anonymize) contribute to breaches of user privacy. In addition, the high volume of personal data, whether disclosed by users or due to the failure of SNS to provide sophisticated privacy tools, has attracted organizations (e.g., GNIP – GNIP Inc. is a social media API aggregation company that provides data from dozens of social media sites). via a single API) to aggregate and sell users' social networks against their data. In addition, the trusted nature of SNS relationships has become an effective mechanism for spreading spam, malware, and phishing attacks. Malicious entities launch various attacks by creating fake profiles, using the guise of stolen SNS accounts that are sold illegally or spreading rumors through bots.

The Internet Security Threat Report (ISTR) states that the increasing use of SNS by hackers cannot be ignored. In 2015 such services turned into a source of spam and malware, and were used as a way to make illegal money on the web. And in 2016, SNS became the main target in identity theft and spear phishing crimes. Research conducted by Rathore et al. [20] confirmed several solutions to prevent these threats. Among them are watermarking, steganalysis and digital oblivion to protect SNS users against threats related to multimedia data. In addition, there are solutions such as spam detection and phishing detection that are offered to overcome traditional threats. And even built-in security solutions such as authentication mechanisms and privacy settings, as well as commercial solutions such as minor monitors and social protection applications are also used to safeguard against both types of threats in SNS.

Research Gao, et al. [21] categorized the main security issues in SNS into four categories (1) privacy issues, (2) viral marketing, (3) network structure based on attacks and (4) malware attacks. Jin et al. studied the behavior of SNS users from four perspectives (1) malicious behavior, (2) mobile social behavior, (3) traffic activity and (4) connections and interactions. Fire et al. [22] divide current security threats into four categories (a) classic threats, (b) modern threats, (c) combined threats and (d) threats targeting children.

With the high use of SNS, the reputation of online users is also increasing through the web. User reputation affects user status and credibility in real life. SNS can damage the reputation of large businesses and organizations, for example, negative posts from employees can damage the reputation of organizations and employees. SNSs are also used by some large companies to form complete profiles of individuals with the aim of selling products and recording individual behavior. But all of this is usually done without the consent of the individual concerned. Additionally, based on Smith's research, 38% of companies spent more than 20% of their advertising budget on SNS in 2015, with Facebook and Twitter displaying the most ads.

Rathore et al. [23] then categorize security threats into three main categories, namely (1) multimedia content threats, data sharing is an important feature in SNS where they can share photos, videos, activities, and interests. Even with advances in multimedia retrieval techniques, such as location estimation, facial recognition, web searches and geotagging, illegal abuse is increasing. Threats of this multimedia content include exposure to multimedia content, ownership sharing, manipulation of multimedia content, steganography, metadata (multimedia content in SNS is metadata because it contains so much important data such as identity and location, for example GPS), multimedia content link sharing, static links, outsourcing and data center transparency, video conferencing, link tagging capabilities of shared multimedia data, and illegal disclosure of data. Category (2) traditional threats, including phishing, malware, sybil attacks and fake profiles, spamming, clickjacking, deanonymization attacks, inference attacks, and profile cloning. Category (3) social threats, including cyberbullying and cybergrooming, corporate espionage, and cyberstalking.

Several solutions offered by Rathore et al. [24] in overcoming SNS security problems include watermarking, co-ownership, steganalysis, digital oblivion, storage encryption, metadata removal and analysis, malware detection, sybil defense and fake profile detection, phishing detection. , spammer detection, commercial solutions, built-in SNS security solutions and cloning profile detection.

These security and privacy issues are continuously being processed to reach an established point and be able to overcome these security and privacy attacks in the SNS world. It is also acknowledged that without legislative support, this negative issue can only be minimized without a comprehensive solution. Henson et al. also offer an alternative to not relying solely on the security features built into network websites, but rather using security and privacy features along with selective scanning criteria in deciding who will allow access to their websites especially with sensitive information.

The founder of Facebook, Mark Zuckerberg once stated his argument when privacy was being questioned on SNS, which in this case was Facebook he created. Mark Zuckerberg has repeatedly stated that his goal is to help people share information more efficiently. By gathering social information and broadcasting it, News Feeds take what people have access to and place it where they care most. Zuckerberg claims that no privacy was compromised in the process. However, Boyd emphasizes, privacy is about how people experience their relationships with other people and with information. Privacy is a sense of control over information, the context in which sharing occurs, and the audience to which it can be accessed.

For this reason, if you look at Boyd's argument, information is not private because no one knows, because it is the individual who makes the limits and controls over it. Boyd also stressed that there is a very large gray area between secrets and information that is meant to be released to the public. Users are unlikely to post secrets, but they often post information that is only relevant in certain contexts. The assumption is that if we visit someone's Facebook page, we can access the information in context. In other words, the main pillar to limit the space and movement of privacy in the context of threats to privacy and data mining on SNS is ourselves.

In the end of his research on privacy on Facebook, Boyd also argues that privacy is not an absolute right - it is a privilege that must be protected socially and structurally in order to always be a primary concern. It is then questioned whether privacy still exists or not is something that is very context dependent on society. Whether people choose to pay attention to this or not.

5. Conclusion

Social Network Sites (SNS) is a type of web service to build a virtual network among people who have similar interests, backgrounds and activities. SNS can be very beneficial to its users as it removes economic and geographic boundaries, and can also be useful in achieving goals related to job search, entertainment and education. The use of SNS encourages a person to disclose personal information (e.g. age, sexual or political orientation, date of birth, purchase of an item, etc.). With the current development of SNS, issues related to how to maintain the privacy and security of users are also starting to emerge, especially when users upload multimedia content such as photos, videos and audio. Henson et al also offer an alternative to not only relying on the security features built into network websites, but rather using security and privacy features along with selective scanning criteria in deciding who will allow access to their websites especially with sensitive information.

Boyd said that information is not private because no one knows, because it is the individual who establishes the boundaries and controls over it. Boyd also stressed that there is a very large gray area between secrets and information that is meant to be broadcast as publicly as possible. Users are unlikely to post secrets, but they often post information that is only relevant in certain contexts. In other words, the main pillar to limit the space and movement of privacy in the context of threats to privacy and data mining on SNS is ourselves. Therefore, apart from taking advantage of the privacy features offered by various SNSs, we need to realize that it is not enough. The assumption is that if we visit someone's Facebook page, we can access the information in context. So, to avoid things like this, it is necessary to protect yourself and in this case it is literacy to be sensitive to privacy on SNS.

This article is expected to contribute to further studies regarding the threat of privacy and data mining in a more complex digital era. By exposing the categories, types, practices, and impacts of privacy and data mining threats in accordance with the conceptual elaboration carried out by the researchers, it is hoped that it can also be a reference for future communication research. The limitations in this study open up new space for further research. This study only describes conceptually how threats to privacy and data mining are in SNS. It will be richer if in the future it raises issues in a more specific geological context. The issue of this threat is actually felt by the people of Indonesia and there are not a few cases that prove this must be considered further. Especially in public literacy to be aware of the dangers and threats to privacy that arise if they are not realized early.

References

[1] D. Liu, P. A. Kirschner, and A. C. Karpinski, “A meta-analysis of the relationship of academic performance and Social Network Site use among adolescents and young adults,” Comput. Human Behav., vol. 77, pp. 148–157, 2017, doi: 10.1016/j.chb.2017.08.039.

[2] A. N. Saiphoo, L. Dahoah Halevi, and Z. Vahedi, “Social networking site use and self-esteem: A meta-analytic review,” Pers. Individ. Dif., vol. 153, no. June 2019, p. 109639, 2020, doi: 10.1016/j.paid.2019.109639.

[3] Q. Zhang, M. Schwade, Y. Smith, R. Wood, and L. Young, “Exercise-based interventions for post-stroke social participation: A systematic review and network meta-analysis,” Int. J. Nurs. Stud., vol. 111, p. 103738, 2020, doi: 10.1016/j.ijnurstu.2020.103738.

[4] S. P. Coundouris, C. L. Tyson, and J. D. Henry, “Social networking site use and relationship quality: A double edged sword,” Comput. Human Behav., vol. 123, no. November 2020, p. 106871, 2021, doi: 10.1016/j.chb.2021.106871.

[5] C. Cheng, Y. ching Lau, L. Chan, and J. W. Luk, “Prevalence of social media addiction across 32 nations: Meta-analysis with subgroup analysis of classification schemes and cultural values,” Addict. Behav., vol. 117, p. 106845, 2021, doi: 10.1016/j.addbeh.2021.106845.

[6] J. Mou and M. Benyoucef, “Consumer behavior in social commerce: Results from a meta-analysis,” Technol. Forecast. Soc. Change, vol. 167, no. July 2020, 2021, doi: 10.1016/j.techfore.2021.120734.

[7] E. J. Ivie, A. Pettitt, L. J. Moses, and N. B. Allen, “A meta-analysis of the association between adolescent social media use and depressive symptoms,” J. Affect. Disord., vol. 275, pp. 165–174, 2020, doi: 10.1016/j.jad.2020.06.014.

[8] A. Fathalizadeh, M. R. Hosseini, A. J. G. Silvius, A. Rahimian, I. Martek, and D. J. Edwards, “Barriers impeding sustainable project management: A Social Network Analysis of the Iranian construction sector,” J. Clean. Prod., vol. 318, no. July, p. 128405, 2021, doi: 10.1016/j.jclepro.2021.128405.

[9] D. Liu and W. K. Campbell, “The Big Five personality traits, Big Two meta traits and social media: A meta-analysis,” J. Res. Pers., vol. 70, pp. 229–240, 2017, doi: 10.1016/j.jrp.2017.08.004.

[10] M. Domínguez-Rodrigo, L. Cobo-Sánchez, J. Aramendi, and A. Gidna, “The meta-group social network of early humans: A temporal–spatial assessment of group size at FLK Zinj (Olduvai Gorge, Tanzania),” J. Hum. Evol., vol. 127, pp. 54–66, 2019, doi: 10.1016/j.jhevol.2018.11.001.

[11] W. Su, X. Han, H. Yu, Y. Wu, and M. N. Potenza, “Do men become addicted to internet gaming and women to social media? A meta-analysis examining gender-related differences in specific internet addiction,” Comput. Human Behav., vol. 113, no. June, p. 106480, 2020, doi: 10.1016/j.chb.2020.106480.

[12] Y. jing Zhang et al., “Social brain network correlates with real-life social network in individuals with schizophrenia and social anhedonia,” Schizophr. Res., vol. 232, pp. 77–84, 2021, doi: 10.1016/j.schres.2021.05.016.

[13] C. Huang, “Social network site use and Big Five personality traits: A meta-analysis,” Comput. Human Behav., vol. 97, no. March, pp. 280–290, 2019, doi: 10.1016/j.chb.2019.03.009.

[14] C. Huang, “Social network site use and academic achievement: A meta-analysis,” Comput. Educ., vol. 119, pp. 76–83, 2018, doi: 10.1016/j.compedu.2017.12.010.

[15] S. Tifferet, “Gender differences in privacy tendencies on social network sites: A meta-analysis,” Comput. Human Behav., vol. 93, no. October 2018, pp. 1–12, 2019, doi: 10.1016/j.chb.2018.11.046.

[16] D. Liu, K. B. Wright, and B. Hu, “A meta-analysis of Social Network Site use and social support,” Comput. Educ., vol. 127, pp. 201–213, 2018, doi: 10.1016/j.compedu.2018.08.024.

[17] S. Yoon, M. Kleinman, J. Mertz, and M. Brannick, “Is social network site usage related to depression? A meta-analysis of Facebook–depression relations,” J. Affect. Disord., vol. 248, no. January, pp. 65–72, 2019, doi: 10.1016/j.jad.2019.01.026.

[18] R. Chen, D. J. Kim, and H. R. Rao, “A study of social networking site use from a three-pronged security and privacy threat assessment perspective,” Inf. Manag., vol. 58, no. 5, p. 103486, 2021, doi: 10.1016/j.im.2021.103486.

[19] B. Bhushan, P. Sinha, K. M. Sagayam, and A. J, “Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions,” Comput. Electr. Eng., vol. 90, no. October, p. 106897, 2021, doi: 10.1016/j.compeleceng.2020.106897.

[20] M. S. Kim, Y. Jung, and J. Kim, “A study on factors affecting privacy risk tolerance to prevent the spread of COVID-19 in South Korea,” Bus. Horiz., no. xxxx, 2021, doi: 10.1016/j.bushor.2021.07.002.