Available online at www.HighTechJournal.org

HighTech and Innovation Journal

ISSN: 2723-9535

Vol. 5, No. 2, June, 2024

Social Media Data Privacy Related to Security Awareness and Student Trust Regarding Data on Instagram

Yohannes Kurniawan [1*], Bella Natalia [1], Windy Pratama [1], Ni Luh Gede Aninda Kesuma Devi [1]

[1] *Information Systems Department, School of Information Systems, Bina Nusantara University, Jakarta 11480, Indonesia.*

Received 27 November 2023; Revised 02 May 2024; Accepted 08 May 2024; Published 01 June 2024

Abstract

Instagram, as one of the most popular social media sites, has brought many new trends. Many people use Instagram to express themselves or share content through photos and videos. While social media data privacy is important, many people still share their daily activities and personal data. This causes a lot of personal information disclosure, which can lead to the potential for crime or misuse of the scattered data, considering that data is crucial today. Therefore, this research was conducted to determine people's social media data privacy and security awareness on Instagram, especially those with a data-related educational background. This research uses quantitative descriptive methods, distributing questionnaires through Google Forms in group chats, personal chats, or questionnaires to respondents directly. The population in this study is made up of students with a computing program background. It also used purposive sampling to determine the number of 153 samples. From the descriptive analysis, it is known that most respondents are aware of the vulnerability of social media data privacy on Instagram. This can be seen from respondents who know what data is used by Instagram, where they also monitor login activity. Respondents also secure their Instagram accounts by not using the same password as other social media accounts. However, in certain cases, some respondents still need to realize this awareness, so education is still needed regarding the importance of social media data privacy, especially on Instagram.

Keywords: Social Media Data Privacy; Awareness; Instagram; Security; Descriptive Statistics.

1. Introduction

Nowadays, social media is frequently used to interact and make contact with others. As of January 2023, social media users accounted for 60.4% of the total population in Indonesia [1]. Instagram is a social networking site that allows users to share pictures and videos of various activities. Based on *DataReportal*, there has been significant growth for almost 60% of Instagram users in the past two years. It was recorded that in January 2022, there were 104.1 million Instagram users in Indonesia, with 37.8% aged 18–24 years, followed by 29.7% aged 25–34 years [2, 3]. It is common for them to be fluent in technology due to their exposure during a period of technological advancements, especially for students with educational backgrounds related to computers and data, such as computing program students at Bina Nusantara University, where the lecture material that students get aims to increase awareness of personal information on social media.

Based on the content people share, Instagram can find out our data, such as our school, office, and even our address, which has a dangerous impact. An easy example is when looking at perfume on an e-commerce platform [4]. When

* Corresponding author: ykurniawan@binus.edu

http://dx.doi.org/10.28991/HIJ-2024-05-02-015

users open Instagram, it shows ads for similar perfumes. It takes work to realize for those with low awareness of disclosing personal information. On August 1, 2020, there was a data leak on Instagram where at least 11.6 million accounts had their personal information exposed. This includes email addresses, phone numbers, account descriptions, and profile photos [5]. Leaked data can be used for fraud, identity abuse, and spam. This is one of the challenges in this research because most social media sites, especially Instagram, require this data to complete a user profile. If the user is not careful when filling in the data, this can cause personal information disclosure. Despite this data leak, many still ignore their personal information.

This gives the perception that education and awareness are needed for students and the public regarding sharing personal information on social media. Based on previous research, these studies mostly discuss awareness of data privacy and disclosure of personal information on social media, with the subjects discussed in this research being Generation Z and internet users. This research focuses on several variables: social media data privacy measured by privacy and security concerns; security awareness measured based on habits, knowledge, and effort when users use Instagram; and information trust measured by the motivation and frequency of Instagram users. Based on the variables determined, this research aims to determine how much awareness and trust students of computing programs have regarding privacy data from social media, especially Instagram. The structure of this paper starts with an introduction, literature reviews, research methods, results and discussions, and conclusions.

2. Literature Reviews

This journal conducted a literature review of previous research to get a theoretical basis to support solving the problem in this research. The theory obtained is the first step to understanding the problem being researched properly. The previous research is shown in Table 1.

Table 1. Literature Review

No.	Title	Year and Methods	Result
1	Pre-service Teachers' Perceptions of Social Media Data Privacy Policies	2021, Descriptive and Interpretive	From the survey results, it can be seen that each respondent must access at least one social media platform every day. Most respondents also stated that they needed to be made aware of the privacy policy regarding using social media for education with their students. Not only that, but the respondents need to become more familiar with the data privacy policies of popular social media services. From the existing problems, it is necessary to have data literacy training in the teacher education program. Researchers encourage teacher educators to consider addressing data privacy beliefs and awareness following a personal data literacy approach where data can be identified, understood, reflected, managed, controlled, and reused for creative applications [6].
2	Case Study on Privacy-Aware Social Media Data Processing in Disaster Management	2020, Research Questions, Group Discussion, Qualitative	This research shows that using the right technology can implement privacy-aware methods to provide social media data processing infrastructure. From this research, VOST members are generally worried about losing important data related to privacy regulations [7].
3	A Comprehensive Study on Privacy and Security on Social Media	2021, Survey Method	Research shows that most respondents are willing to share information with others without hesitation. However, most are unwilling to share their data with social media service providers. This research also found that the privacy concerns on social media websites are very weak, and the efforts of users to make practical enhancements to their social media privacy are much lower than other modes of security operation. In addition, many social media users need more technological skills, which results in lower privacy concerns about their posts [8].
4	Legal Framework Governing Social Data Analytics and Privacy Concerns among Social Media Users	2019, Literature Review	This research aims to identify privacy concerns related to social media and the laws governing the protection of personal information. No matter the complexity of data protection and privacy on social media, there is still the possibility of violations of the use of personal information by third parties, so it cannot reach total individual privacy on social media unless it refrains from sharing personal data across social networking services. Therefore, regulations are important in eradicating uninformed consent from social media users [9].
5	A Critical Analysis in Understanding the Impact of Privacy and Security Towards Social Media Among Young Adults	2022, Sampling Method	This study aims to understand the impact of privacy and security on social media among young adults. The analysis results show that 33.3% of respondents strongly agree that security and privacy can be a major concern in social media. Social media security and privacy have always been an issue, and care must be taken to protect personal data from cyber-attacks. Therefore, it is hoped that social media can focus more on protecting user data effectively. Respondents must implement new measures to control cyber-attacks or malware that can impact user confidentiality [10].
6	The Urgency of Doxing on Social Media Regulation and the Implementation of Right to be Forgotten on Related Content for the Optimization of Data Privacy Protection in Indonesia	2022, Descriptive	This research shows that the privacy rights of doxing victims in Indonesia have not been comprehensively protected. This is because Indonesia still needs proper and specific doxing regulations on social media. Unlike Indonesia, Singapore and Hong Kong already have special regulations for doxing actors on social media. Therefore, Indonesia can observe these two countries in making regulations for doxing actors on social media [11].
7	Awareness of the Use of Social Media Among Students: Malaysia and Indonesia	2022, Quantitative Method	The study results show that the level of transparency in sharing personal data of Indonesian students is lower than that of Malaysian students. In addition, Indonesian students are also more open to showing their email addresses compared to Malaysian students [12].
8	Awareness of Social Media Privacy Among the Staff at Solo Sokos Hotel Lahden Seurahuone	2021, Qualitative Method	The results of the data analysis show that the awareness of staff at Solo Sokos Hotel Lahdden Seurahuone about social media privacy is below average. Staff needed to be made aware of the available privacy settings provided by social media. Given the existing problems, staff should be able to increase their awareness of privacy on social media [13].
9	''Why Should I Read the Privacy Policy, I Just Need the Service'': A Study on Attitudes and Perceptions Toward Privacy Policies	2021, Quantitative Method	The survey results show that more than 50% of respondents need help understanding the content of the privacy policy provided. Most respondents are also concerned about the type of data service providers collect. Users often do not understand the risks associated with accepting a privacy policy, resulting in loss of privacy. This raises concerns about how service providers use privacy policies to tailor personal data lawfully [14].

10	Everybody wants some: Collection and Control of Personal Information, Privacy Concerns, and Social Media Use	2021, Quantitative Method	Social media is growing to the point where social media is always used in daily activities. This raise concerns in the community about the security of personal data on social media. Several studies yielded results in a straight line with the theory of privacy calculus, whereby people generally put personal information aside when it is of greater benefit to them. This study indicates that men pay more attention to control and access to their personal information and lower levels of social media use. This is based on the current demographic, where most women will spend more time using social media than men [15].
11	Privacy Risk Awareness and Intent to Disclose Personal Information of Users Using Two Social Networks: Facebook and Instagram	2022, Convenient Sampling Method	This research shows that social media users have high trust in social media, for example, Facebook and Instagram, when users have a low view of the security risks. However, users will feel anxious when their personal data is used for promotion. So, this research concludes that when someone is used to sharing information on trusted social media platforms, awareness of data privacy risks will be low. In contrast, those who have experienced problems with data privacy will be very careful in sharing information in any form [16].
12	The Effects of Privacy Awareness, Security Concerns and Trust on Information Sharing in Social Media among Public University Students in Selangor	2022, Quantitative Method	This research informs that students will feel increasingly worried about the security of social media itself. With this worry, students' trust in social media will have an impact. It is known that with high trust, it will be easier for someone to share personal information on social media. Therefore, when someone is given information or education about the security of their data on social media, users will have a feeling to reduce the sharing of their data. Even though several security guarantees are provided, it still does not change someone's feeling of insecurity when sharing information on social media [17].
13	Privacy and Security Information Awareness and Disclosure of Private Information by Users of Online Social Media in the Ibadan Metropolis, Nigeria	2023, Descriptive Survey Research	Based on this research, most Facebook social media users need to be aware of their data, which many people can easily see. This could be due to the need for more education about personal data privacy and security on social media. However, some are already educated about the importance of their data. For them, using authentication is one technique that can be used to protect their data from being spread. Privacy and security awareness greatly influence how individuals disseminate their personal information. Those aware of the risks and have a good education will increase the security of their information [18].
14	Methods to Prevent Privacy Violations on The Internet on the Personal Level in Indonesia	2023, Literature Review	This research shows that there are several reasons why privacy violations occur, namely the existence of malicious software that causes programs on computers to be easily accessible by viruses and the like. In addition, Online Social Networking can easily leak someone's data. OSN is one of the most vulnerable ways for someone's data to spread across the internet. The last cause is a phishing attack where users are lured to open a link that traps them into providing their data. Some methods can be done by installing Computer Security Software to increase the security of a system. Then, there is training for end-user awareness so that users can be aware and easily scan the causes of violations of personal information [19].
15	Effect of Penitence on Social Media Trust and Privacy Concerns: The Case of Facebook	2020, Quantitative Method	This study explains that the existence of violations regarding users' data on a social media platform can affect how social media users act. When Facebook found itself in this privacy data breach problem, it apologized to retract its users. The release of this apology allowed Facebook to regain its integrity, but users remained concerned about their personal information [20].
16	Social Media Privacy Concerns, Security Concerns, Trust, and Awareness: Empirical Validation of an Instrument	2021, Quantitative Method	This research shows that respondents who are students with student backgrounds who are in an information technology major feel that privacy concerns are felt when students do not have control over the data on the internet. Trust in software is affected by its privacy and security, so its users are highly aware of the risks that can occur [21].
17	The Effect of Perceived Privacy, Security, and Trust on the Continuance Intention to Use Social Networking Services (A Study on Meta's Social Networks)	2022, Quantitative Methods (Descriptive Approach)	This study shows that perceived privacy, security, and trust increase the desire to use SNS. When users have full trust and know the security of SNS, users will unconsciously use this SNS continuously. However, SNS has tricks to convince users that it has good security so that user privacy data does not spread. This trick creates another thought in the user's heart regarding using their private data [22].
18	Evaluating Security and Privacy Issues of Social Networks-Based Information Systems in Industry 4.0	2021, Data Sampling, Sentiment Analysis, Latent Dirichlet Allocation, Textual Analysis	This research studies that there are concerns about social networking systems, especially those that are interconnected in Industry 4.0. Connecting many devices to a system can cause an inadvertence from the security system, which makes it easy for third parties to access data on a platform. This results in the company's internal information being easily seen, which can be detrimental because it can be an advantage for companies in one sector. Therefore, further learning is needed to improve the security of all connected devices regarding system security and human resource management [23].
19	Indonesian University Students' Awareness in Using Online Transportation Systems Based on Data Privacy and Risk Factors Perspective	2023, Purposive Sampling Method	From this study, information was obtained that students who have been using the Online Transportation System for a long time will pay more attention to how OTS companies use their data, whether used in promotions or otherwise. Those who are old users will trust OTS companies more for their data storage than new users. This study also states that most women will tend to believe what the company claims, but both women and men are aware of the risks that can occur [24].
20	How to Address Data Privacy Concerns When Using Social Media Data in Conservative Science	2020, Qualitative Method	The research results show that social media data is increasingly used in conservation science to study human-nature interactions. Of course, there is a legal basis for using this data, such as regulations for using social media data and regulations for processing personal data. This is because if the data is misused, many risks can arise, such as damaging one's reputation and the risk of criminal liability. Possible mitigation strategies that can also be carried out to help reduce the impact of this risk are using data protection such as depreciation and pseudonymization [25].
21	Indonesian Generation Z's Awareness of Data Privacy in the Use of Social Media	2022, Quantitative and Descriptive Statistics	The results of this study indicate that most of Generation Z is quite aware of the importance of social media data privacy. This can be seen from using social media passwords, which are quite complex (9 - 15 characters). In addition, most of the Z generation also use something other than unknown public networks (Wi-Fi), and only a few use public devices. Most Generation Z who uses public devices always ensure to log out of all accounts before leaving the device. However, the number of Generation Z aware of the importance of social media data privacy is similar to those unaware of it. Most of them use the same password on each social media. Some use personal information as a password [26].
22	Users' Awareness of Personal Information on Social Media: Case on Undergraduate Students of Universitas Indonesia	2020, Qualitative Method	This study's results show how social media users' awareness is related to personal information on their social media. Most participants or users of social media already know what personal information is, can explain the types of personal information, and know the importance of personal information. This is very important because, in social media, there is the potential for misuse of personal information, which is closely related to privacy. This research also suggests that social media users have sufficient knowledge about the use of social media [27].

23	Awareness of Data Privacy on Social Networks by Students at Qassim University	2020, Questionnaire and Random Sampling Method	This study shows how awareness regarding information privacy among students at Qassim University uses social media. Most respondents use social media such as WhatsApp, Snapchat, Facebook, Twitter, and Instagram. From the results of this study, most students at Qassim University already have an awareness of privacy and personal information. Students ensure that their privacy is maintained, and that personal information is not shared. This can be seen from several actions, such as setting alarms for login activity, limiting profile visibility, and blocking spam users. Students also mostly use social media to interact with friends and prevent contact with new people for security reasons [28].
24	Is Somebody Spying on Us? Social Media Users' Privacy Awareness	2020, Questionnaire and Convenience Sampling Method	This study shows the results of an analysis related to students' digital privacy awareness in using social media and how this awareness affects them in using social media. Compared to male students, female students are more aware of the risks of social media, so female students prefer to share some of their personal information. However, both of them have sufficient awareness of the security of social media privacy because students already know there is a risk that third parties can use information shared on social media at any time [29].
25	The Social Media Dilemma: Millennials Dealing with Data Tracking in a Mediatized Society	2021, Qualitative, Semi-Structured Interviews, and Focus Groups	The results of this study indicate that data tracking, which allows personalization of services for each user, can endanger individual privacy, and most millennials feel a dilemma regarding data tracking on the social media being used. Millennials have become aware of the importance of their personal information on social media. However, despite this sense of dilemma, users continue to use social media due to the importance of social media today in society [30].
26	Personal Advertising on TikTok: How Aware Is Generation Z Regarding Their Data that is Being Collected by TikTok for Personal Advertising?	2023, Quantitative Method	The results of this study show how social media, especially TikTok, maintains the privacy data of its users and how Generation Z is aware of this. Most Generation Z know that TikTok uses its data for personalized advertising. However, in reality, this research shows that Generation Z, in general, only knows 25% of the data collected by TikTok, so it can be concluded that Generation Z does not yet have full awareness of the importance of their data [31].
27	Student Attitudes, Awareness, and Perceptions of Personal Privacy and Cybersecurity in the Use of Social Media: An Initial Study	2020, Survey Method (Quantitative)	This study's results indicate that some students, especially students at the University of Western Pennsylvania, have used security features for their social media to reduce existing privacy security risks. However, some students still feel that it is okay if third parties use their data. However, most students know about privacy and security risks when using social media. There are several ways to prevent privacy risks when using social media, including setting social media account passwords with complex passwords, managing account visibility, and using two-factor authentication [32].
28	Examining University Students' Online Privacy Literacy Levels on Social Networking Sites	2021, Quantitative Method	This research shows that increased use of social media can increase the risk of privacy security issues. In addition, researchers can also find out how student behaviour is related to privacy security on social networking sites / social media. It can be seen that female students have a higher level of Online Privacy Literature (OPL) than male students; therefore, female students are more aware of the importance of personal information data on social media [33].
29	We Care About Different Things: Non-Elite Conceptualizations of Social Media Privacy	2019, Quantitative and Descriptive Analysis	This research shows that users prioritize horizontal privacy (privacy between users) over vertical privacy (freedom from surveillance). This has implications for privacy regulations and the role of institutional players in protecting user privacy. It is also known that there are power imbalances and gaps in perceptions of privacy based on gender and wealth. Overall, this research emphasizes the need for a multidimensional understanding of privacy and the importance of considering user perspectives in privacy research and regulation [34].
30	Cybervetting and the Public Life of Social Media Data	2020, Quantitative and Verificative Analysis	This research aims to see how the growing use of social media to screen job applicants can affect people's trust in organizations that engage in this practice. It can be noted that privacy boundaries are important not only when it comes to personal information but also information publicly available on social media. This research identifies that just because social media data is public, it does not mean that people do not have context- and data-specific privacy expectations [35].

Based on previous research, most of these studies discuss privacy, data awareness, and the disclosure of personal information on social media. Most of the subjects discussed in this study are Generation Z and internet users. Previous research helped us know the awareness of research subjects to private data on social media, where some subjects had awareness regarding the importance of private data. However, some subjects have quite low awareness. Researchers also understand the important aspects that must be considered in protecting data privacy, such as paying attention to application terms and conditions, changing passwords regularly, and considering risks before uploading personal information to social media. Based on the previous research, researchers agree on the importance of awareness when uploading personal information on social media. The indicators needed in this research can also be found in the research researchers conducted in previous studies. This research will discuss awareness and trust among the School of Information Systems and School of Computer Science students at BINUS University who are close to and knowledgeable about the data. Here, researchers also apply descriptive analysis to find out more clearly about the awareness and trust of the subjects.

3. Research Methods

This study used a quantitative descriptive method by distributing a survey to a predetermined sample through a Google Forms questionnaire. The quantitative descriptive method is a research method that defines and draws conclusions based on events that can be studied and uses numbers without testing a hypothesis [36]. This journal used purposive sampling, where, at this stage, researchers have determined the research subjects, namely students from the BINUS University computing programs, namely the School of Information Systems and the School of Computer Science. The data collection process was performed in approximately a month, from July 3 to August 11, 2023, through group classes, personal chat with the subject determined, or distributing questionnaires to the person directly.

The questionnaires are based on predetermined variables and indicators, with the respondents choosing multiple-choice or checkbox answers. Descriptive analysis is used to process the results of the questionnaire. Descriptive analysis is a method used to describe the data collected. This method is used to test respondents to see their awareness of disclosing personal information and sensitivity to social media data privacy. The methods of this research are displayed in Figure 1.

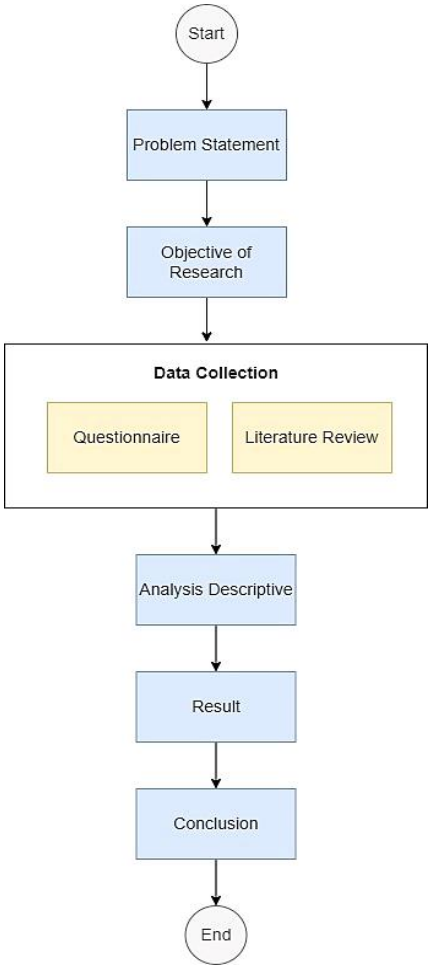

Figure 1. Research Method

Following is a list of questions that will be used in the questionnaire in this research (Table 2):

Table 2. Variables and Questions

Variable	Indicator	Definition	Question	Choice of Answers
Social Media Data Privacy	Privacy concern (PC)	Privacy issues that exist on Instagram, such as the use of personal data for corporate (marketing) purposes [28]	(PC01) What type of Instagram account do you have?	• Public • Private
			(PC02) What do you do if there is privacy policy information on Instagram?	• Did not read it entirely • Reading but ignoring it • Always read and care
			(PC03) Do you feel disturbed if third parties use your data?	• Yes • No
	Security concern (SC)	Security issues such as identity theft and malware attacks [21]	(SC01) How do you control privacy security on Instagram?	• Two-factor authentication • Change password regularly • Monitoring login activity • Not doing anything
			(SC02) What do you do if you find an account in the name of a relative?	• Block • Report • Restrict (manage interactions with other accounts)

Security Awareness	Behaviour (BE)	Habits of students in using social media, especially Instagram [26]	(BE01) Do you often log into Instagram accounts on other people's devices?	• Often • Rarely • Never
			(BE02) Do you always log out of Instagram after logging in on other people's devices?	• Yes • No
	Knowledge (KL)	Student's knowledge related to personal information security [26]	(KL01) Are you aware of the possibility of hijacking Instagram accounts?	• Yes • No
			(KL02) Are you aware of the potential for malware attacks on Instagram?	• Yes • No
			(KL03) Do you know what kind of personal data Instagram collects?	• Profile Information (Name, Profile Picture, Bio, Uploaded Contents) • Contact (email address and phone number) • Search activities and interaction (like, comment, and message) • Geographic location • Device Data (type of device and operation system)
			(KL04) Do you know how Instagram uses users' data?	• Targeted ads • Increasing user experience • User analysis • Sharing data with third parties
			(KL05) Which shows the misuse of privacy data on Instagram?	• Using location feature • Targeted ads with our interests • Fake account • Tag a friend in a post
			(KL06) In your opinion, is the behaviour in the image below the right thing to do? *) Write addresses, cell phone numbers, and emails on Instagram accounts publicly	• True • False
			(KL07) In your opinion, is the behaviour in the image below the right thing to do? *) Join the "Add Yours" sticker trend with personal information	• True • False
			(KL08) How do you find a fake account on Instagram?	• Number of followings and followers • Number and context of posts • Bio and profile picture • Profile Username
	Effort (EF)	Efforts made by students to maintain the security of personal data [26]	(EF01) How do you create an Instagram account password?	• Combination of letters and numbers with a length of 6 characters (Binus1) • Combinations of letters, numbers, and symbols with more than six characters (b!Nu$12)
			(EF02) Does your Instagram account use the same password as other social media?	• Yes • No
Trust of Information	Motivation (MV)	Student's motivation in uploading personal information on social media [28]	(MV01) What is your goal when uploading content on Instagram?	• Share and capture moments • Seeking attention • Job-related
	Frequency (FQ)	The intensity of how much personal information is uploaded by students on social media [28]	(FQ01) How often do you upload content on Instagram?	• Everyday • Once every two weeks • Once a month • Rarely to never count

Researchers can perform quantitative analysis to determine how factors, such as the type of data shared, the social media platform used, or the user's level of privacy awareness, affect data privacy by employing well-defined variables and indicators. The variables and indicators employed in this study were selected based on earlier studies. Prior research enhances our understanding of students' awareness of social media data privacy. Based on the variables and questions in Table 2, Of the 153 respondents, 71.2% were male, and 28.8% were female, with the largest age range, namely 17-22 years, which amounted to 98%, and an age range of 23 -28 years old, which amounts to 2% of the total respondents. Then, 75.8% of the total respondents were students with a School of Information Systems (SIS) background, 22.9% of the total respondents were students with a School of Computer Science (SoCS) background, and the remaining 1.3% students were not in both SIS and SoCS.

4. Result and Discussion

The data obtained is analyzed using descriptive analysis methods to gain insight into an event assisted by percentage measurements. Based on the data collected, as many as 98.7% were Instagram users, and 1.3% were not Instagram users. From here, it can draw information where most respondents were Instagram users and were familiar with Instagram's features.

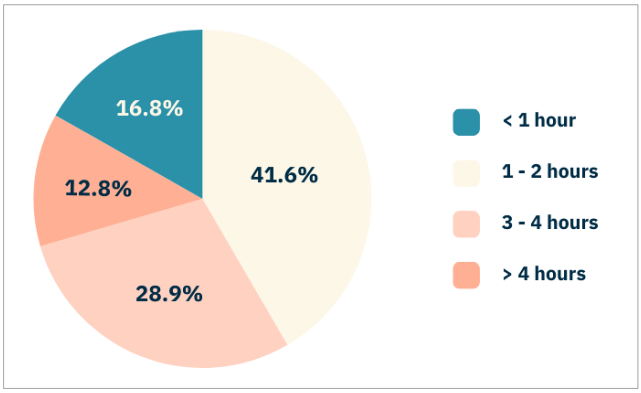

Figure 2. Instagram Usage Time

From the questionnaire results shown in Figure 2, most respondents (41.6%) use Instagram daily for around 1 - 2 hours. Meanwhile, 12.8% of respondents used Instagram for more than 4 hours daily. Generation Z spends 79% of their time accessing social media, including Instagram. The latest data from Google Consumer Behavior, states that Indonesia, with a total population of 265.4 million, has 50% of social media users.

Figure 3. Total Instagram Accounts

Based on Figure 3, most respondents have two or only one account. Supported by data from Data Reportal, the number of social media users in Indonesia at the start of 2022 shows that there are 68.9% of the total population. It supports the figure above that one person can have two or more accounts, especially as Instagram occupies the second position on the ranking of frequently used social media platforms.

Table 3. Instagram Account Type

	Responses Number	PC01 Proportion
Private	92	61.7%
Public	57	38.3%
Total	**149**	**100%**

Based on Table 3, from the accounts owned by respondents, it can be seen that 61.7% have private Instagram accounts. In other words, the activities of these Instagram accounts cannot be seen by anyone. Meanwhile, 38.8% of respondents have a public Instagram account.

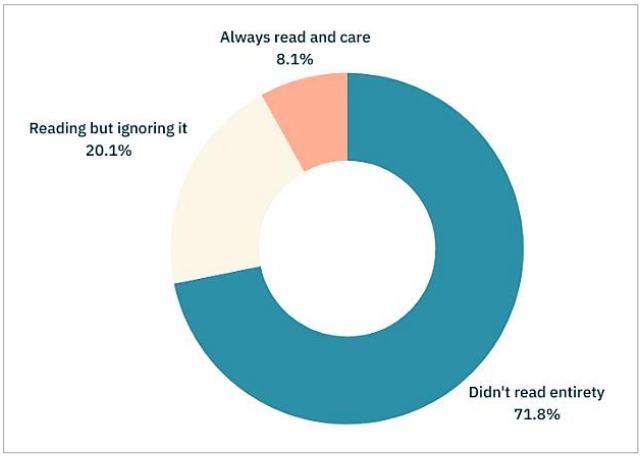

Figure 4. Privacy Policy Information on Instagram

Figure 4 shows that 71.8% of respondents did not read the privacy policy information during initial Instagram registration. Only 8.1% of respondents always read and care about policies on Instagram. This information is directly proportional to the journal "Concerned Enough to Act? Privacy Concerns & Perspectives Among Undergraduate Instagram Users", which states that most people consider the privacy policies on social media to be too long and complicated, so it is difficult to invest their time and energy in reading these privacy policies.

Table 4. Use of Data by Third Parties

	Responses Number	PC03 Proportion
Yes	123	82.6%
No	26	17.4%
Total	**149**	**100%**

From Table 4, as many as 82.6% of all respondents said that they were bothered because they considered the data used to be a form of privacy, and they did not know what the data would be used for by third parties. However, 17.4% of all respondents said they were not bothered or had no problem if third parties used their data. Awareness of the importance of data is crucial because if our data is misused, this could lead to potential cybercrime that utilizes information technology and can cause harm to victims affected by the crime.

Table 5. Controlling Privacy on Instagram

	N Valid	Missing
SC01	149	4

The privacy security on our Instagram account is very important to protect our account from external threats. In Table 5, it can be seen that there are four missing data because the respondents needed to meet the criteria.

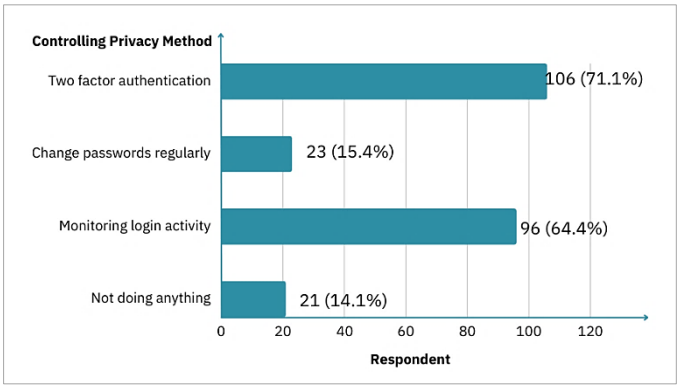

Figure 5. Controlling Privacy on Instagram

As seen in Figure 5, most respondents control the privacy security of their Instagram accounts by using Two Factor Authentication in line with monitoring their login activity. Doing 2FA is to protect their Instagram account from cyber criminals, which frequently happens. Instagram uses 2FA to protect its users by sending a code through text message if there is an unrecognized login attempt. On top of that, they also control privacy security by changing their password frequently. However, some respondents do nothing to control their Instagram accounts' privacy security.

Table 6. Action When Found Fake Account Instagram

	N Valid	Missing
SC02	149	4

Table 6 shows four missing data because two respondents were not students with computing program backgrounds, and two more did not use Instagram.

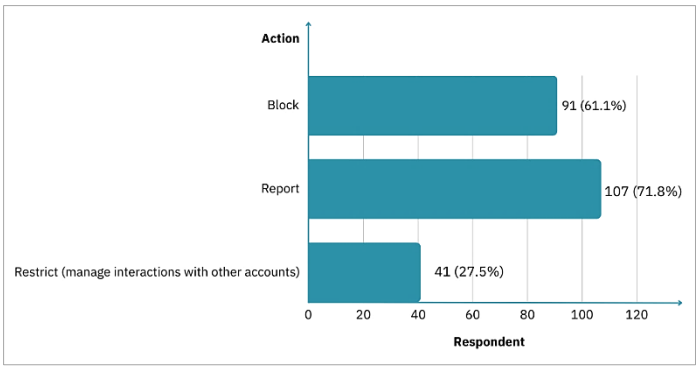

Figure 6. Action When Found Fake Account Instagram

Figure 6 shows that most respondents will report if users find an unknown account in the name of a relative. Instagram has also recommended that blocking and reporting are the actions that can be done if an account is impersonating someone. When someone reports the account, they can tell which account the fraudster is pretending to be. Restricting is also one of some respondents' actions to limit their interaction with fake accounts.

Table 7. Frequency of Login to Instagram Accounts on Other People's Devices

	Responses Number	BE01 Proportion
Often	2	1.3%
Rarely	67	45%
Never	80	53.7%
Total	**149**	**100%**

The users can log on to Instagram accounts from various devices, such as cell phones, tablets, PCs, and laptops. Based on Table 7, 53.7% of all respondents have never logged in to an Instagram account on someone else's device, 45% said that they rarely log in to their Instagram account on someone else's device, and only 1.3% often log in on other people's devices. Of the respondents, 90.4% always log out, and 9.6% did not log out after logging in on someone else's device. Logging in on someone else's device and not logging out could lead to data misuse for crimes, resulting in huge losses.

Table 8. Awareness of Account Hijacking

	Responses Number	KL01 Proportion
Yes	146	98%
No	3	2%
Total	**149**	**100%**

Based on the results of the questionnaire distributed, Table 8 shows the numbers that have very significant differences. 98% of respondents know and are aware of the possibility of account hijacking, while 2% are unaware. This tells us that almost all respondents are aware of the dangers that will occur on social media, especially Instagram.

Table 9. Potential Malware Attacks

	Responses Number	KL02 Proportion
Yes	138	92.6%
No	11	7.4%
Total	**149**	**100%**

A malware attack describes software that can damage a device or system. The way it is spread can be through phishing emails, malicious advertising links, and others. Based on Table 9, as many as 92.6% of the respondents were aware of the potential for malware attacks on Instagram. However, as many as 7.4% of the respondents were unaware of the potential for malware attacks on Instagram.

Table 10. Use of Password on Social Media Accounts

	Responses Number	EF02 Proportion
Yes	62	41.6%
No	87	58.4%
Total	**149**	**100%**

And to protect our data, especially on Instagram accounts, one of the basic things that can be done is through a password. Users can prevent unwanted people from accessing our data or Instagram accounts with passwords. Table 10 shows that 58.4% have Instagram account passwords that differ from other social media passwords. Meanwhile, 41.6% still use the same Instagram account password as other social media passwords.

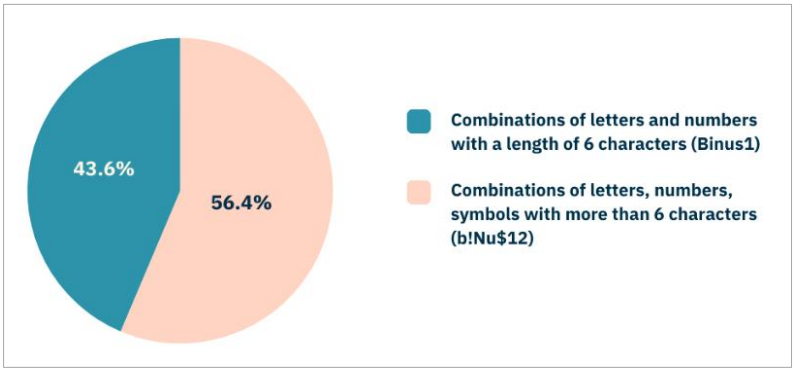

Figure 7. Instagram Account Password Combination

Apart from that, the combination of passwords they use can also be seen in Figure 7, where as many as 56.4% use passwords with letters, numbers, symbols, and more than six characters long. However, as many as 43.6% still use passwords that only contain a combination of letters and numbers and are six characters long. Users' limitations could influence these results in creating new password combinations, so some choose to use the same password for every social media account they have. This can also be influenced by the effort required to remember the password used for each social media account [37].

Table 11. Purpose of Uploading Instagram Content

	N Valid	Missing
MV01	149	4

Instagram can be used for all purposes, from personal to business. Some personal purposes are to contact relatives and friends or see current trends. The business needs in question include benchmarking against competing companies. As seen in Table 11, there are four missing data because the respondent did not meet the criteria.

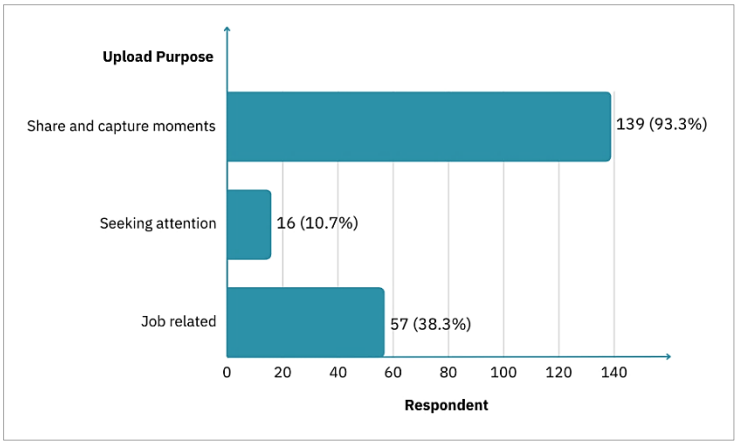

Figure 8. Purpose of Uploading Instagram Content

Figure 8 shows that most respondents (93.3%) uploaded content to their Instagram accounts to share and keep the moments. The moment can be a birthday celebration, graduation celebration, family gathering, or outing content at the workplace. In addition, 38.3% of respondents were using Instagram to upload content for job-related purposes and 10.7% of respondents were uploading content as an attempt to seek attention.

Table 12. Types of Data Collected by Instagram

	N Valid	Missing
KL03	149	4

Table 12 shows four missing data because two respondents were not students with computing program backgrounds, and two were no longer using Instagram.

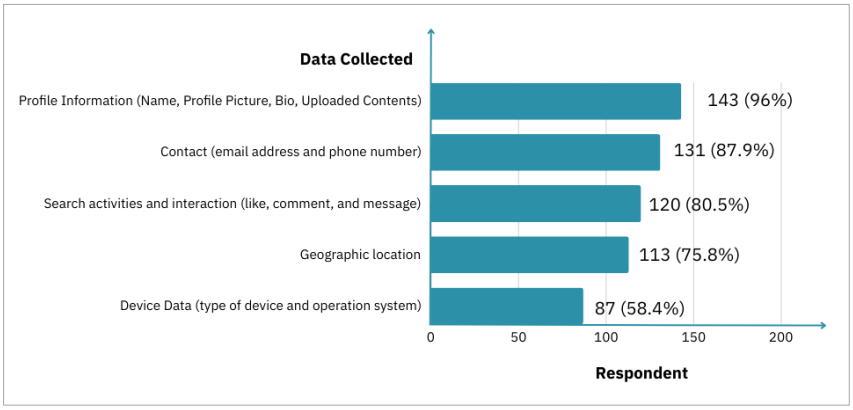

Figure 9. Types of Data Collected by Instagram

Figure 9 shows that respondents know that Instagram collects personal data through profile information (name, profile photo, bio, and uploaded content), contact, searching and interaction activities, geographic location, and device data. However, most respondents must know that Instagram collects device data such as device type and operating system. The factor influencing respondents answers that users must upload information such as email, telephone number, name, and others when registering.

Table 13. How Instagram Uses User Data

	N Valid	Missing
KL04	149	4

This value was obtained by calculating the number of responses to questions about the purpose of using personal data on Instagram, which 149 respondents answered out of 153 total respondents. Table 13 shows four missing data because two respondents were not students with computing program backgrounds, and two were no longer using Instagram.

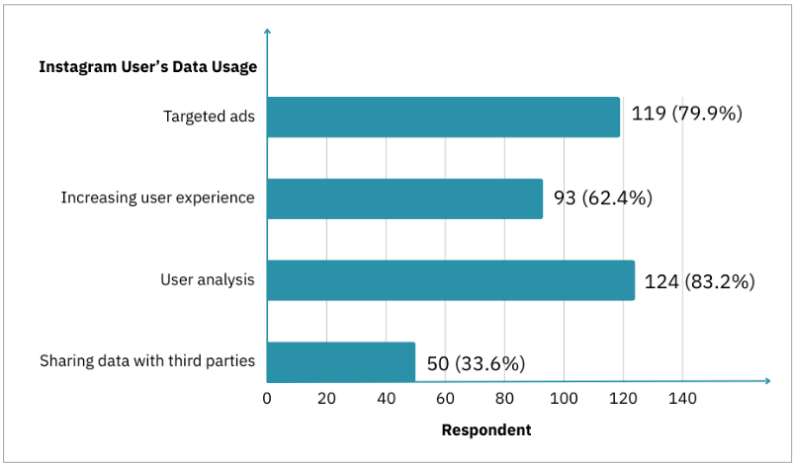

Figure 10. How Instagram Uses User Data

From Figure 10, most respondents know that Instagram uses its users' data for customized advertising, user analysis, and increased user experience. Factors influencing respondents' answers are impacts that users can feel directly. This can be seen when users often get advertisements and recommendations on Instagram that have been adjusted to the demand and the demographics of Instagram users. 33.6% of the respondents also notice that Instagram uses their data to share them with third parties.

Table 14. Misuse of Privacy Data on Instagram

	N Valid	Missing
KL05	149	4

Table 14 shows four missing data because two respondents were not students with computing program backgrounds and two were no longer using Instagram.

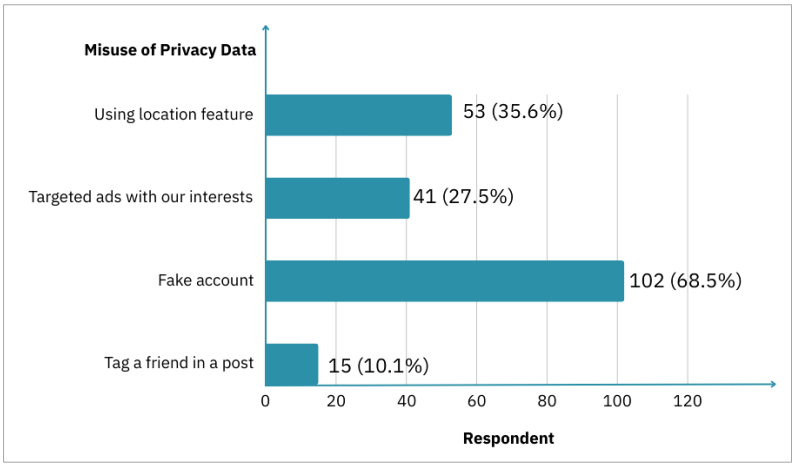

Figure 11. Misuse of Privacy Data on Instagram

Based on Figure 11, respondents are aware of fake accounts on Instagram. In this case, a fake account takes personal data from other Instagram users and uses that account to commit criminal acts. Sometimes, users who create fake accounts in the name of other people deliberately commit violations such as writing malicious comments or uploading bad posts to bring down other people's names. There is another misuse of privacy data on Instagram, such as the location feature that can be used to track our location, customized advertising, and tagging a friend in a post, which could track our location and the person tagged.

Table 15. Case of Dissemination of Personal Data on Instagram

	Responses Number	KL06 Proportion
Yes	38	25.5%
No	111	74.5%
Total	**149**	**100%**

Based on Table 15, in cases where someone wrote their address, cell phone number, and email in the description of their Instagram account publicly, 74.5% stated that this was not the right thing to do. However, 25.5% of the total respondents stated that sharing personal information publicly on Instagram was correct or not dangerous. This case differs from what is appropriate because writing the address, cell phone number, and email in the account description means users have distributed their data or information, which certain people can misuse.

Table 16. "Add Yours" Case

	Responses Number	KL07 Proportion
Yes	23	15.4%
No	126	84.6%
Total	**149**	**100%**

The feature "Add Yours" has become a trend on Instagram recently, where Instagram users can use it to share their beautiful moments. However, some Instagram users unconsciously use this feature to share their data, such as personal ID, date of birth, and signature. From Table 16, it can be seen that 84.6% said that sharing personal data through the "Add Yours" is wrong, and as many as 15.4% said this action was not dangerous to do.

Table 17. Fake Account Case

	N Valid	Missing
KL08	149	4

As shown in Table 17, there were four missing data because two respondents were not students with computing program backgrounds, and two were no longer using Instagram.

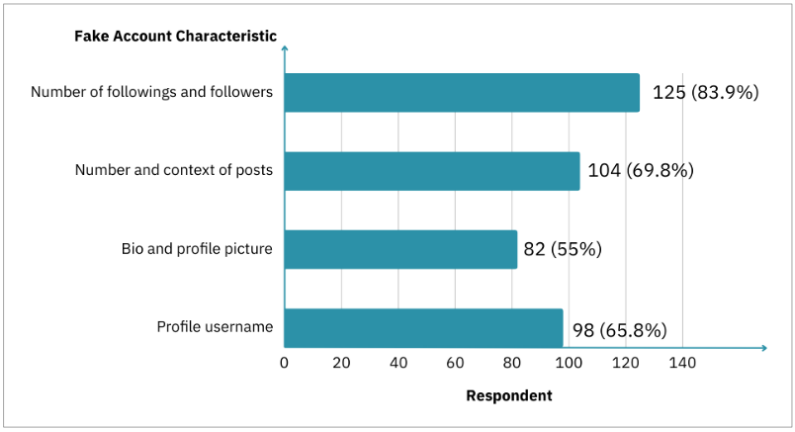

Figure 12. Fake Account Case

As shown in Figure 12, respondents also found out about fake accounts in 4 ways: by looking at the number of followers and following, the content of posts from an account, username profile, bio, and profile picture. Fake accounts will be easily detected when users know the username contains the names of people they know. All the factors in the answer choices above can also detect fake accounts.

Based on the results we have analyzed, students with a computing background, especially at Bina Nusantara University, can discover what data is used by Instagram, how to secure our accounts and cases related to data privacy. This study is in line with previous research which discusses Generation Z that they were aware of data privacy on social media, where the respondents in this study were also part of Generation Z. Students' awareness does not rule out the possibility that several per cent of them are still unaware of data privacy on Instagram. Likewise, with the terms and conditions provided by Instagram, most respondents felt that the terms and conditions provided could have been clearer, so they chose to ignore this. High awareness of data privacy on Instagram would be better accompanied by reading the terms and conditions.

5. Conclusion

This research aimed to identify the awareness and trust of computing program students at Bina Nusantara University regarding data privacy on Instagram. With several indicators tested, it is known that most respondents are Instagram users with a frequency of 1-2 hours per day. Through this research, it is known that respondents are aware of the

importance of data privacy on Instagram. This can be seen by respondents who know that their data is used by Instagram, such as email, cell phone numbers, and activity data, where this data is used for customized advertising and user analysis. Although respondents were aware of Instagram's use of their data, most respondents avoided reading the privacy policy because they found it too long and complicated to understand. The privacy policy is very important because it contains crucial information regarding the activities carried out in the application.

Even so, most respondents still control the security of their account privacy by monitoring login activities, such as never logging in to their Instagram account on someone else's device and always logging out of their account if they log in on someone else's device. They also use two-factor authentication, so other people cannot easily log in to their Instagram accounts. According to the research, respondents secure their accounts using different passwords for each social media account. The password used is a combination of letters, numbers, and symbols with a length of more than six characters. With this, they can avoid account hijacking and malware attacks. In conclusion, future research should carry out tests by providing education regarding data privacy cases such as malware attacks so that the level of awareness of data privacy increases Considering nowadays, many people use social media because of social demands or following trends, so they prefer to be trendy over the security of their privacy and security.

6. Declarations

6.1. Author Contributions

Conceptualization, Y.K., B.N., W.P., and N.L.G.A.K.D.; methodology, Y.K., B.N., W.P., and N.L.G.A.K.D.; software, Y.K., B.N., W.P., and N.L.G.A.K.D.; formal analysis, Y.K., B.N., W.P., and N.L.G.A.K.D.; resources, Y.K., B.N., W.P., and N.L.G.A.K.D.; data curation, Y.K.; writing—original draft preparation, B.N., W.P., and N.L.G.A.K.D.; writing—review and editing, Y.K.; visualization, B.N., W.P., and N.L.G.A.K.D.; supervision, Y.K.; project administration, B.N., W.P., and N.L.G.A.K.D.; funding acquisition, Y.K. All authors have read and agreed to the published version of the manuscript.

6.2. Data Availability Statement

The data presented in this study are available in the article.

6.3. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

6.4. Institutional Review Board Statement

Not applicable.

6.5. Informed Consent Statement

Not applicable.

6.6. Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

7. References

[1] We Are Social. (2023). Special Report: Digital 2023 Your ultimate guide to the evolving digital world. We Are Social Website, Jakarta, Indonesia. Available online: https://wearesocial.com/id/blog/2023/01/digital-2023/ (accessed on March 2024)

[2] NapoleonCat. (2024). Instagram Users in Indonesia - January 2023. Napoleoncat.com, Ontario, Canada. Available online: https://napoleoncat.com/stats/instagram-users-in-indonesia/2023/01/ (accessed on March 2024).

[3] NapoleonCat. (2023). Instagram users in Indonesia - August 2023. Napoleoncat.com, Ontario, Canada. https://napoleoncat.com/stats/instagram-users-in-indonesia/2023/08/ (accessed on March 2024).

[4] Janssen, D. (2023). What Does Instagram Know About Me? VPNOverview.com, Nijmegen, The Netherland. Available online: https://vpnoverview.com/privacy/social-media/what-does-instagram-know-about-me/ (accessed on March 2024).

[5] Winder, D. (2021). 235 million Instagram, TikTok and YouTube user profiles exposed in massive data leak. Forbes, New Jersey, United States. Available online: https://www.forbes.com/sites/daveywinder/2020/08/19/massive-data-leak235-million-instagram-tiktok-and-youtube-user-profiles-exposed/?sh=420099be1111 (accessed on March 2024).

[6] Marín, V. I., Carpenter, J. P., & Tur, G. (2021). Pre-service teachers' perceptions of social media data privacy policies. British Journal of Educational Technology, 52(2), 519–535. doi:10.1111/bjet.13035.

[7] Löchner, M., Fathi, R., Schmid, D. ‘. L., Dunkel, A., Burghardt, D., Fiedrich, F., & Koch, S. (2020). Case study on privacy-aware social media data processing in disaster management. ISPRS International Journal of Geo-Information, 9(12), 9 12, 709. doi:10.3390/ijgi9120709.

[8] Albulayhi, M. S., & El Khediri, S. (2022). A Comprehensive Study on Privacy and Security on Social Media. International Journal of Interactive Mobile Technologies, 16(1), 4–21. doi:10.3991/IJIM.V16I01.27761.

[9] Mansour, Y. R. (2019). Legal Frameworks Governing Social Data Analytics and Privacy Concerns among Social Media Users. Lebanese American University, Beirut, Lebanon. doi:10.26756/th.2020.159.

[10] Unni, M. V, & Jeevananda, S. (2022). A Critical Analysis in Understanding the Impact of Privacy and Security Towards Social Media Among Young Adults. The Seybold Report Journal, 17(11), 454–461. doi:10.5281/zenodo.7316177.

[11] Yudiana, T. C., Rosadi, S. D., & Priowirjanto, E. S. (2022). The Urgency of Doxing on Social Media Regulation and the Implementation of Right to Be Forgotten on Related Content for the Optimization of Data Privacy Protection in Indonesia. Padjadjaran Jurnal Ilmu Hukum, 9(1), 24–45. doi:10.22304/pjih.v9n1.a2.

[12] Isa, K., Sam, T. H., Palpanadan, S. T., Diniaty, A., Munthe, R. A., Vasudevan, A., & Subramaniam, G. (2022). Awareness of The Use of Social Media Among Students: Malaysia and Indonesia. The Seybold Report, 17(6), 1140–1152.

[13] Bhatt, Y. (2021). Awareness of social media privacy among the staff at Solo Sokos Hotel Lahden Seurahuone. LAB University of Applied Sciences, Lahti, Finland.

[14] Ibdah, D., Lachtar, N., Raparthi, S. M., & Bacha, A. (2021). Why Should I Read the Privacy Policy, I Just Need the Service’: A Study on Attitudes and Perceptions Toward Privacy Policies? IEEE Access, 9, 166465–166487. doi:10.1109/ACCESS.2021.3130086.

[15] Cain, J. A., & Imre, I. (2022). Everybody wants some: Collection and control of personal information, privacy concerns, and social media use. New Media and Society, 24(12), 2705–2724. doi:10.1177/14614448211000327.

[16] Minh, D. T., Ly, P. T. T., & Duyen, N. T. N. (2022). Privacy Risk Awareness and Intent to Disclose Personal Information of Users Using Two Social Networks: Facebook and Instagram. VNU University of Economics and Business, 2(6), 1-10. doi:10.57110/vnujeb.v2i6.133.

[17] Ara, A., Zainol, Z., & Duraisamy, B. (2022). The Effects of Privacy Awareness, Security Concerns and Trust on Information Sharing in Social Media among Public University Students in Selangor. International Business Education Journal, 15(2), 93–110.

[18] Omotayo, F. O., & Olayiwola, J. O. (2023). Privacy and Security Information Awareness and Disclosure of Private Information by Users of Online Social Media in the Ibadan Metropolis, Nigeria. The African Journal of Information Systems, 15(1), 1-26.

[19] Ismail, H., Febiyanto, F., Kevin, & Moniaga, J. V. (2022). Methods to prevent privacy violations on the internet on the personal level in Indonesia. Procedia Computer Science, 216, 650–654. doi:10.1016/j.procs.2022.12.180.

[20] Ayaburi, E. W., & Treku, D. N. (2020). Effect of penitence on social media trust and privacy concerns: The case of Facebook. International Journal of Information Management, 50, 171–181. doi:10.1016/j.ijinfomgt.2019.05.014.

[21] Koohang, A., Floyd, K., Yerby, J., & Paliszkiewicz, J. (2021). Social media privacy concerns, security concerns, trust, and awareness: Empirical validation of an instrument. Issues in Information Systems, 22(2), 133–145. doi:10.48009/2_iis_2021_136-149.

[22] Riache, H., & Pradana, M. (2022). The Effect of Perceived Privacy, Security, And Trust on The Continuance Intention to Use Social Networking Services (A Study on Meta’s Social Networks). Jurnal Pemikiran Dan Penelitian Bidang Administrasi, Sosial, Humaniora Dan Kebijakan Publik, 5(2), 102–108.

[23] Saura, J. R., Ribeiro-Soriano, D., & Palacios-Marqués, D. (2022). Evaluating security and privacy issues of social networks-based information systems in Industry 4.0. Enterprise Information Systems, 16(10–11), 1694–1710. doi:10.1080/17517575.2021.1913765.

[24] Susilahadi, R., Yasirandi, R., & Utomo, R. G. (2023). Indonesian University student’s awareness in using online transportation system based on data privacy and risk factors perspective. AIP Conference Proceedings, 2654. doi:10.1063/5.0117515.

[25] Di Minin, E., Fink, C., Hausmann, A., Kremer, J., & Kulkarni, R. (2021). How to address data privacy concerns when using social media data in conservation science. Conservation Biology, 35(2), 437–446. doi:10.1111/cobi.13708.

[26] Adrian, N., Lindawaty, D. F., & Kurniawan, Y. (2023). Indonesian Generation Z’s Awareness of Data Privacy in the Use of Social Media. International Conference of Industrial Engineering and Operations Management Istanbul, 1693–1703. doi:10.46254/an12.20220318.

[27] Iman, R. N., Asmiyanto, T., & Inamullah, M. H. (2020). Users’ Awareness of Personal Information on Social Media: Case on Undergraduate Students of Universitas Indonesia. Library Philosophy and Practice, 2020, 1–11.

[28] Alabdulatif, A., & Alturise, F. (2020). Awareness of data privacy on social networks by students at Qassim University. International Journal of Advanced Computer Research, 10(50), 194–205. doi:10.19101/ijacr.2020.1048094.

[29] Deniz, Ş. (2019). Is Somebody Spying on Us? New Media and Visual Communication in Social Networks, 156–172. doi:10.4018/978-1-7998-1041-4.ch009.

[30] Volman, H. (2021). The Social Media Dilemma: Millennials Dealing with Data Tracking in a Mediatized Society. Uppsala Universitet Department of Informatics and Media, Uppsala, Sweden.

[31] Hussein, A., Sivac, A., Arguioui, H. E., & Diehl, J. (2023). Personal advertising on TikTok: How aware is generation Z regarding their data that is being collected by TikTok for personal advertising? In Academic Competencies for Information Management 2022-2023, 1-13. doi:10.5281/zenodo.7520169.

[32] Bhatnagar, N., & Pry, M. (2020). Student Attitudes, Awareness, and Perceptions of Personal Privacy and Cybersecurity in the Use of Social Media: An Initial Study. Information Systems Education Journal, 18(1), 48–58.

[33] Kaya, S., & Yaman, D. (2021). Examining University Students' Online Privacy Literacy Levels on Social Networking Sites. Participatory Educational Research, 9(3), 22–45. doi:10.17275/per.22.52.9.3.

[34] Quinn, K., Epstein, D., & Moon, B. (2019). We Care About Different Things: Non-Elite Conceptualizations of Social Media Privacy. Social Media and Society, 5(3), 1-14. doi:10.1177/2056305119866008.

[35] Gruzd, A., Jacobson, J., & Dubois, E. (2020). Cybervetting and the Public Life of Social Media Data. Social Media and Society, 6(2), 1-13. doi:10.1177/2056305120915618.

[36] Mbuva, G. (2023). Quantitative descriptive research: definition, types, methodology, methods, characteristics, examples, and advantages. Available online: https://www.accountingnest.com/articles/research/quantitative-correlational-research (accessed on March 2024).

[37] Madnick, S. E. (2020). Do You Have Password Headaches? You Are Not Alone, and It Is Unnecessary! Working Paper CISL# 2020-14, 1-3. doi:10.2139/ssrn.3555448.