sustainability

MDPI

Article

Analysis of Higher Education Students' Awareness in Indonesia on Personal Data Security in Social Media

Yohannes Kurniawan [1], Samuel Ivan Santoso [1], Regina Rolanda Wibowo [1], Norizan Anwar [2], Ganesh Bhutkar [3] and Erwin Halim [1,*]

[1] Information Systems Department, School of Information Systems, Bina Nusantara University, Jakarta 11480, Indonesia
[2] School of Information Science, College of Computing, Informatics and Media, Universiti Teknologi MARA, Shah Alam 40450, Malaysia
[3] Centre of Excellence in HCI, Vishwakarma Institute of Technology, Pune 411037, India
* Correspondence: erwinhalim@binus.ac.id

Abstract: As time goes by, information and communication technology continue to advance. Since the pandemic, the need for information and communication technology has risen to aid us in working and studying from home. One of the forms of information and communication technology is social media. Social media is where users can connect with other users in different regions, upload content as images or videos, express themselves freely, and get responses or reactions from other users (likes and comments). However, behind all those, social media can also be a place full of threats towards the personal data of its users. This study aims to analyze the awareness of higher education student social media users in the research field of Indonesia regarding personal data security. This research focuses on university students, Indonesia's largest group of social media users, as the main respondents. The questionnaire questions were distributed online using random and snowball sampling methods for targeting student respondents. In this study, social media users were divided into active users (content creators) and passive users (using social media as a means of entertainment). The results show that active users upload personal data to benefit from it. In contrast, passive users are more aware of the use of personal data on their social media. This research also shows how they secure their data and their behavior on social media.

Keywords: personal data; security; social media; awareness; higher education student; information security

Citation: Kurniawan, Y.; Santoso, S.I.; Wibowo, R.R.; Anwar, N.; Bhutkar, G.; Halim, E. Analysis of Higher Education Students' Awareness in Indonesia on Personal Data Security in Social Media. *Sustainability* **2023**, *15*, 3814. https://doi.org/10.3390/su15043814

Academic Editors: De-Chih Lee and Chih-Chien Wang

Received: 14 December 2022
Revised: 2 February 2023
Accepted: 5 February 2023
Published: 20 February 2023

1. Introduction

The ongoing pandemic has changed how we perform activities or work. Everything that was previously performed directly offline is now migrating to online activities. This change triggers the need for online applications that can be used within our daily activities; these include social media. Social media can be defined as an online platform that can accommodate all forms of content in the form of images or videos sent by social media users. Most social media can be downloaded for free and can be directly used by anyone as long as they are connected to the internet.

The number of new users on social media continues to increase, as is triggered by the COVID-19 pandemic in 2019. Indonesia is one country with a fairly high number of active social media users. According to Hootsuite (We Are Social), active social media users in Indonesia in 2019 reached 130 million, or 48% penetration of the total population of Indonesia at that time, namely, 268.2 million [1]. Then, in 2022, Hootsuite (We Are Social) again uploaded data on the number of active social media users in Indonesia, which was around 191.4 million, or 68.9% of the total population of Indonesia, which was recorded as 277.7 million [2]. Both data show that the number of active social media users from 2019 to 2022 increased by 61.4 million, or around 47.2%. Other data showing the number of active social media users in Indonesia come from the Indonesia Internet Service Providers

Association or *Asosiasi Penyelenggara Jasa Internet Indonesia* (APJII); the data obtained show that the internet penetration rate in Indonesia in 2021 until Q1 of 2022 reached 77%, namely, 210,026,769 people from a total population of 272,682,600 in 2021 [3]. Other data on the number of active social media users in Indonesia differentiated by age groups are 8.3% aged 0–4 years, 13.9% aged 5–12 years, 8.2% aged 13–17 years, 11.6% aged 18–24 years, 14.9% aged 25–34 years, 14.7% aged 35–44 years, 12.7% aged 45–54 years, 9.0% aged 55–64 years, and 6.8% aged 65 years and over [4]. According to APJII, the levels of active social media users in Q1 2022, if grouped by age, were 8.08% aged 5–12 years, 9.62% aged 13–18 years, 25.68% aged 19–34 years, 27.68% aged 35–54 years, and 5.97% aged 55 years and over [3].

Data obtained on the active social media users in Indonesia show that the age group that accesses social media the most is the 18–34 age group. Therefore, our research objective is higher education students who fall into this age group, being one of the groups that frequently use social media. Students use social media as a tool to find various information, or just a place to find entertainment or express themselves. However, behind those, there is a hidden threat in social media, such the theft of personal data, either intentionally or unintentionally, consciously or unconsciously. This issue raises the main concern of our research, as to whether students are aware of personal data security on social media.

Usually, identity theft on personal data occurs when the data are circulated everywhere, such as images, videos, or text written in content on social media. One case is the "Add Yours" challenge trend that went viral on Instagram Indonesia. "Add Yours" is an Instagram feature that can be used freely by its users by uploading it on their Instagram Story; if their Story is public, then other users can see it, and other users are also free to upload their own. All Instagram users can see the data collected in "Add Yours", so many people exploit this. Then, they commit fraud by creating "Add Yours" regarding ID card photos, photos of themselves with ID cards, nicknames, addresses, mothers' names, birth dates, and other personal data. Unfortunately, many users quickly upload the personal data mentioned earlier, and the total number of participating users can reach up to tens of millions [5].

The case mentioned above can be categorized as social engineering, because obtaining personal data involve the psychological manipulation of users who think it is a challenge or trend [6]. The case continues until financial fraud occurs, where some criminals use personal data to contact the owner and pretend to be close relatives, family, friends, or spouses. After that, the perpetrator starts to borrow money for various reasons, and finally, the victim gives the money because he believes that the acquaintance is someone close [5]. The case mentioned above has indeed occurred on social media; other cases take the form of uploading personal data on social media in the form of pictures or videos, such as identity cards, ATM cards, house numbers, telephone numbers, places that are being occupied, and so on, which can be uploaded either intentionally or unintentionally.

Personal data security and social media are interrelated because the protection of personal data is important when using or accessing social media. Research related to this matter comes from several aspects or areas that are different from each other, and can also describe the conditions of social media users in a country. In this case, Lawrence Ryz et al. (2016) mentioned the evolution of a basic rule regarding data protection, namely, GDPR [7]. Radi Romansky (2014) discussed the challenges that can be faced by a social media company in maintaining the privacy of each of its users [8]. Users trust robots or Siri in providing personal data [9]. Gender plays a role in making choices to share personal data [10]. The use of social media in the health sector and the usage decisions of each user have been differentiated based on work function or role in the health sector [11]. Some research uses psychological factors to make a person pursue a higher level of security but pay the appropriate price for it [12]. There are factors affecting feelings of trust in social media [13], or FOMO attitudes [14]. In addition, location factors influence a person's concern for the security of their personal data [15]. Our research contributes to updating and providing an understanding of the conditions of social media users in Indonesia in understanding the importance of the security of their personal data. We cover users at a young age who are

the largest users in Indonesia, and these can be represented by higher education students. In this study, we divide social media users into two groups, namely, active and passive, because both of them have different views on protecting or sharing their personal data with other users through their social media accounts. Based on previous explanations, this research explores students' awareness levels of personal data security on social media. This research aims to increase the awareness of personal data security and provide an overview of the factors influencing students to upload their data, the level of current awareness, and the security measures taken. The sections of this research paper are organized as follows:

1. Provides a literature review as the foundation of our research.
2. Provides the research method, data analysis and results.
3. Summarizes the essence of the research we have conducted.

2. Literature Review

2.1. Personal Data

Personal data are a part of the data that resides on a computer or mobile device [16]. According to the General Data Protection Regulation (GDPR), personal data are information about an identifiable individual. An identifiable person can be identified, directly or indirectly, by reference to an identification number or one or more factors specific to their physical, physiological, mental, economic, cultural, or other social features [17].

Personal data that can be used directly to identify an individual can be categorized as Personally Identifiable Information (PII) [16]. Personally Identifiable Information (PII) may include name, date of birth, home address, gender, race, phone number, email address, political opinions, credit card number, health information, ID cards, IP address, and location data [17]. Hence, personal data are the main asset for social media, because they can be used for business or other developer purposes [18,19].

2.2. An Overview of Rules and Regulations for Personal Data Protection

Personal data security protects personal data and information from the possibility of unauthorized access, disclosure, disruption, deletion, corruption, modification, or destruction [20].

As mentioned by Sylwia Kosznik-Biernacka [21], personal data should be protected and secured based on the CIA triad:

- Confidentiality—The required degree of protection of the information against unauthorized access;
- Integrity—Data and information should be correct, intact, and not be manipulated;
- Availability—Data are available under the system or user requirements.

Related rules or regulations on personal data security are included in GDPR, a regulation in the European Union law on data protection and privacy in the European Union and the European Economic Area. Though it was originally published for the scope of the European Union, and is one of the world's toughest privacy and security laws, the regulation has had influence and become a great reference for many organizations and countries worldwide [17].

There are some related standards that discuss personal data security, such as [22] provides a way to protect valuable information using the base standard of ISMS (Information Security Management System), whereas [23], established by the ISACA (Information Systems Audit and Control Association), provides guidance or a framework for managing enterprise information and technology that supports enterprise goal achievement.

In Indonesia, on 20th September 2022, the UU PDP (*Undang-Undang Perlindungan Data Pribadi*) or local personal data protection law was officially formalized. The UU PDP aims to protect Indonesia's citizens' data and sets a standard for legally processing and maintaining data. The UU PDP was drafted based on the reference of the GDPR [24].

2.3. Functions and Threats for Personal Data Security Associated with the Use of Social Media

The use of social media has continued to increase since the COVID-19 pandemic; social media is used to share and get the latest information about the pandemic, such as diagnostic, treatment, hospital location, total infected, and follow-up protocols [25]. Another use of social media is to build personal branding by updating personal information. Some believe a personal brand will help them create a good reputation or career on social media [26].

In terms of personal branding, many social media users began to utilize social media as a place for them to seek fame and start their focus as a celebrity or content creator in various ways, one of which is uploading their data in the form of images, videos, or text [27]. Regarding images and videos, a study shows that visual content can increase the number of views and likes, rather than just plain text; of course, the average image or video contains photos of the user and their activities [28], or even travel experiences [29]. The most frequent reason for a user to upload their data is the psychological need to get attention, or simply as a way to express themselves [30].

As explained earlier, personal data consist of several data types that refer to an individual. Social media users can sort out which data can be shared. Some users agree that phone numbers and home addresses are the most sensitive personal data and should not be made public, while other personal data are made public by some users [31].

Using personal data on social media can expose a person to becoming known to many people, but foremost, it poses cyber threats to users' personal data. Cyber threats may appear in the following forms [32].

A. Burglary

Robberies do not only occur online, as criminals seek victims through social media. Social media is where users can share information by posting; one example is daily activities. Criminals easily find the target they want through social media by paying attention to their daily activities. After that, the perpetrator only needs to pay attention to the valuables included in the post; then, the criminals can plan to steal the valuables.

B. Social Engineering

Social Engineering uses psychological manipulation to obtain personal data. Thus, the victim will unconsciously provide their data. Some examples include, for example, a call on behalf of a close relative or a message from a friend or relative. Usually, this type of social engineering is based on a goal that can be the theft of personal or financial information.

C. Phishing

Phishing is one of the crimes that can occur on social media. Phishing aims to trick the victim into giving their data. Phishing is usually done by sending a message to the victim containing a gift, on the condition that they provide personal data first with the reason being to verify the receipt of the gift. In addition, phishing can also take the form of a replica that resembles the address of a well-known website or institution that offers special offers or gifts to victims. Usually, phishing occurs on social media, which has the feature of allowing the sending messages either to each individual or in groups.

D. Malware

Malware is software specifically designed to damage other devices without the device owner's knowledge, and it can enter easily via attachments, messages, and links.

E. Identity Theft

Identity theft is a crime that uses someone's data for certain purposes without the permission of the owner of the personal data. Thus, any losses that may occur will be accepted by the actual owner of the information, such as losses in terms of finances, debts, loans, and so on. Social media is the best place to mine personal data because many users unknowingly upload it. One example is TikTok, a social media platform that provides short video-based content. Several TikTok videos lead to the leakage of personal data, such as

the "Private school check" video, which others can use to find the user's school name and look for other information such as name, age, gender, date of birth, and address.

F. Cyber-Stalking

Stalkers in the cyber world using social media or other online media can cause irritation, harassment, and emotional anxiety in victims. Stalkers usually do not target the victim's valuables, but seek attention and commit immoral verbal acts. The stalkers will continuously see what the target is doing by looking at the posts uploaded by the target.

G. Cyber-Casing

Cyber-casing is a process used to mark or generate locations in the real world using various data types on social media. This can be done because of the features offered by social media that are intended for users who want to mark their location, perhaps while taking a picture; this feature is known as geo-tagging. Some social media already has this feature and continues to grow to the point of sharing live s, so that other users can monitor location movements using the live location feature. This threat can occur if a criminal sees and begins to mark the location points usually visited by their target, so that the perpetrator can commit a crime in the right place.

Apart from cyber-attacks that target users' data, there are other threats, such as the misuse of a person's data to attack the owner of the data on social media, such as uploading content that embarrasses or humiliates a person, tracking down a person and then physically attack the person, blackmail, bullying, discrimination, torture, commercial advertising, racism [33], and some sexual violence such as nudity content (images or videos of a person undressing), threats of rape, sex messaging, and other types of sex crimes [33,34].

2.4. Factors Influencing Personal Data Security Awareness

Personal data security awareness can be defined as the knowledge of security measures that can be taken to protect personal data on social media. Several things that can affect the level of awareness are age, education level, security training obtained [35], the level of psychosocial health of each user, FoMO behavior [14], or the level of user trust in social media, usually due to perceived enjoyment, benefits obtained, and status [13].

A study has been conducted to analyze user behavior in submitting personal data voluntarily; this study has concluded that users trust online agents such as robots or Siri to deliver personal data online, rather than giving it to human agents directly [9]. Another study analyzed the influence of gender on personal data security awareness and found that gender also influences the decisions made by each user to open their data [10]. Country location factors can also affect this level of awareness; this is evidenced by research conducted in Iraq and Turkey, which concluded that Iraq has a higher level of vulnerability than Turkey [15].

The security awareness level of social media users related to their data can be considered quite low due to several factors mentioned earlier. Some studies have also concluded that although younger users have a higher level of security than older users [35], there are still young users who can be quite vulnerable, because they do not know how to increase security either in general, such as using privacy settings [36], or setting strong password combinations [37]. Indonesia has a low level of security awareness amongst smartphone users, such as the results of storing important data on smartphones and installing illegal applications into them [38]. Throughout all these studies, it has been noted that there is no previous research that analyzes the level of personal data security awareness amongst higher education students (largest age group of social media users) in Indonesia. Therefore, this research will focus on analyzing the level of security awareness regarding personal data on social media amongst Indonesian students by dividing them into two types of social media users—active users (someone who actively create and shares content/information in the form of photos, videos, text, or other things that can be loaded on social media)

and passive users (someone who spends time on social media looking for information, contacting relatives, friends, or entertain themselves) [39].

3. Method

3.1. Research Model

Our research focuses on showing how higher education students are aware of personal data security when on their respective social media. Figure 1 describes our research model, along with each hypothesis.

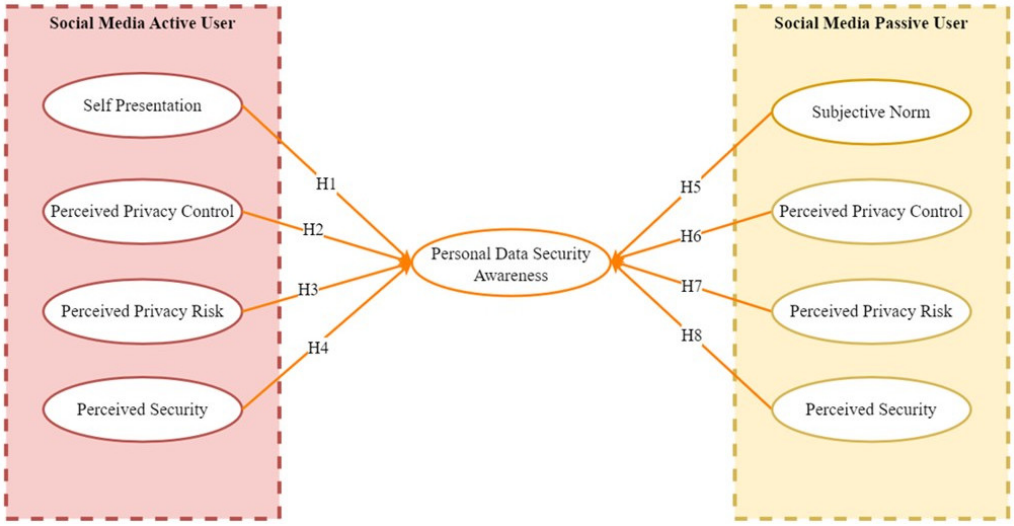

Figure 1. Research model.

3.2. Research Method

This study was conducted using a quantitative method with random and snowball sampling, which involved distributing questionnaires. The sampling types were combined to gather a wider range of higher education students from various universities in Indonesia. Snowball sampling was conducted to gather data from the author's base university and random sampling was conducted to gather data from other universities via other campus' group chats. Our main criteria for respondents were for higher education students who use various social media platforms such as Instagram, TikTok, Facebook, Twitter, LinkedIn, and so on. Respondents ranged from the age of 18 to 24. The respondents were divided based on the type of social media user that they selected on our questionnaire, and the Likert scale used for each question ranged 1–4 (ranging from 1 = "Strongly Disagree" to 4 = "Strongly Agree"). The data were collected using Google Forms through various social media platforms, including Instagram, Line, and WhatsApp. The data were analyzed and interpreted using SmartPLS (p and T Value). Table A1 in Appendix A is the list of questions that we included on our online questionnaire.

3.3. Hyphothesis Development

3.3.1. Effect of Self-Presentation on Personal Data Security Awareness

Self-presentation can be interpreted as a behavior or action taken by someone, meaning social media users adjust or introduce themselves to the public [30]. Self-presentation can also be interpreted as a way to be recognized or accepted by others, especially in social media. Self-presentation can influence a person to share personal data on their social media, to get a certain benefit [30]. In this case, some users upload photos of themselves, their activities, or even their lifestyles on social media [26]. Therefore, we can conclude that self-presentation can adversely affect personal data security awareness.

H1: *Self-presentation harms personal data security awareness in active social media users.*

3.3.2. Effect of Perceived Privacy Control on Personal Data Security Awareness

Perceived privacy control is a person's ability to collect, change, and use personal data [27]. In this case, when someone knows that they do not have full control over their data on social media, that person will choose not to upload any personal data and take other security measures to ensure that the data do not leak. According to [27], perceived privacy control does not influence someone to upload or not upload their personal data on social media. In this study, perceived privacy control is summarized as follows.

H2: *Perceived privacy control positively impacts personal data security awareness in active social media users*.

H6: *Perceived privacy control positively impacts personal data security awareness in passive social media users*.

3.3.3. Effect of Perceived Privacy Risk on Personal Data Security Awareness

Perceived privacy risk is the understanding of each user regarding the privacy risks they can experience while using social media [27]. Perceived privacy risk can influence someone not to upload their data to social media because they already understand what risks can occur [27,30]. Therefore, we summarize the perceived privacy risk below.

H3: *Perceived privacy risk has a positive impact on personal data security awareness in active social media users*.

H7: *Perceived privacy risk has a positive impact on personal data security awareness in passive social media users*.

3.3.4. Effect of Perceived Security on Personal Data Security Awareness

Perceived security is about the level of user trust in the provided or guaranteed social media security [30]. Therefore, there are cases wherein users neglect the security of their own accounts by ignoring the security measures they can take.

H4: *Perceived security has a negative impact on personal data security awareness in active social media users*.

H8: *Perceived security has a negative impact on personal data security awareness in passive social media users*.

3.3.5. Effect of Subjective Norm on Personal Data Security Awareness

Subjective norm is about a person's behavior as regards taking action when considering things that may judge them; usually, the judgement will come from the people closest to the individual [10,31]. In this case, people with this will usually be more careful in uploading content on social media.

H5: *Subjective norm has a positive impact on personal data security awareness in passive social media users*.

4. Results and Discussion

4.1. Measurement Model

The research instrument's reliability was assessed using two measures: the composite reliability (CR) and Cronbach's alpha. The value for both measures is 0.5 or above [27]. In Tables 1 and 2, there are several constructs with values that have exceeded the predetermined limits.

Table 1. Demographics of respondents.

Statement	Item	Frequency
Type of social media users	Active	106
	Passive	98
The most used social media	Youtube	35
	Whatsapp	34
	Facebook	1
	Instagram	78
	TikTok	31
	Line	8
	Twitter	11
	Reddit	1
	Pinterest	0
	Tumblr	1
	Discord	4

Table 2. Mean value for active user.

Construct	Items	Mean
Perceived Privacy Control	PPC01	2.575
	PPC02	2.594
	PPC03	3.255
Perceived Privacy Risk	PPR01	3.264
	PPR02	3.434
	PPR03	3.019
	PPR04	3.547
Perceived Security	PS01	2.792
Self-Presentation	SP01	2.377
	SP02	2.066
	SP03	2.104
Personal Data Security Awareness	PDS01	3.085
	PDS02	2.679
	PDS03	2.226
	PDS04	3.085
	PDS05	1.840
	PDS06	3.113
	PDS07	3.472
	PDS08	3.594

4.2. Questionnaire Results

Through the questionnaire, we collected a total of 204 respondents over 24 days, since our questionnaire was distributed through social media platforms. The collected respondents comprise 106 active social media users and 98 passive social media users, which can be seen in Table 1.

The results of the questionnaire from Table 3 will also be interpreted in the form of horizontal bar charts for each variable shown by the two types of social media users; this aims to display the differences in answers between the two types of users.

Item descriptions based on the diagram above:

- PPC01—We ask our respondents whether they have read and understood each point contained in the Terms of Service on the social media they are currently using. Active users have a higher average score than passive users;
- PPC02—Questions about the understanding of privacy policies on social media used by both types of users. Active users read and understand privacy policies more often than passive users;

- PPC03—In this section we asked for statements about users' understanding of the loss of control over data shared on social media. Passive users have a higher average score than active users;
- PPR01—Data submitted to social media will certainly be stored and used by the developer for various purposes, which have been conveyed previously through the Terms of Service. Passive users have a higher average value than active users;
- PPR02—Social media accounts that are also connected to applications or other third parties will be able to provide access to developers to open or use data on other accounts that are directly connected to our social media accounts. Active users have a higher average value than passive users.
- PPR03—The data shared on social media, especially on the social media profile, can be accessed and stored by other users if they get permission from us. Active users have a higher average value than passive users;
- PPR04—Personal data threats on social media are very diverse, as explained earlier. In this section, we ask each respondent if they know at least one of the various forms of attacks on their personal data. Passive users have a higher understanding compared to active users;
- PS01—Each social media platform certainly has its own features and security levels, set to ensure the security of each user. In this section, we ask about our respondents' level of security trust in the social media they use. Passive users have a higher level of trust than active users;
- PDS01—A password is required to create an account on any social media, and this password aims to be the main protector of account security and account verification when logging in on any device. Every social media platform asks its users to use a combination of numbers, characters, and uppercase and lowercase letters when creating a password, but only a few users use the combination. Active users use a unique password combination more often than passive users;
- PDS02—The passwords we use may be reused for other accounts. In this section, we asked about the use of different passwords for each account owned by the user. Active users use different passwords more often than passive users;
- PDS03—The password stored can be changed according to the user's will. This aims to prevent the password from being easily guessed by others. Active users change their passwords more often than passive users;
- PDS04—Two-factor authentication is one form of security effort offered by social media. The way it works is that users need to enter an OTP (one-time password) or code sent by social media to the email or phone number that has been connected to the social media account every time the user logs in on a new device. Active users activate two-factor authentication for each account more often than passive users;
- PDS05—Each social media platform provides an option for users to log out of their accounts at any time. The aim of this is to increase account security, because then every other person who accesses the social media platform needs to enter a password again before being able to open a social media account. Active users log out more often than passive users;
- PDS06—Every social media platform has a privacy feature that is useful for regulating who can see the content contained in each user's account. Of course, this can help users control the spread of data on social media. Both types of users have a good understanding of, and use, this privacy feature, because the average difference between the two is not too far;
- PDS07—In this section, users are given statements related to uploading personal data on their social media accounts, and some of them feel that they have never uploaded their personal data;
- PDS08—Personal data that have been circulated on social media will be difficult to change or delete. This happens because some other users may have stored the data in

the local storage of their devices. Passive users have a higher level of understanding about this than active users.

Table 3. Mean value for passive user.

Construct	Items	Mean
Perceived Privacy Control	PPC01	2.327
	PPC02	2.449
	PPC03	3.480
Perceived Privacy Risk	PPR01	3.378
	PPR02	3.316
	PPR03	2.888
	PPR04	3.622
Perceived Security	PS01	2.908
Subjective Norm	SN01	3.449
	SN02	2.173
	SN03	2.714
Personal Data Security Awareness	PDS01	2.816
	PDS02	2.306
	PDS03	1.724
	PDS04	2.847
	PDS05	1.582
	PDS06	3.122
	PDS07	3.388
	PDS08	3.673

As shown in Table 4, the majority of the Cronbach α values were more than 0.500, following the benchmarked score of 0.500, and these can be accepted as reliable [27]. The construct of "Self-Presentation" scored more than 0.900, which means that the data collected have high reliability. Since the construct of "Perceived Security" factors contains only one single item, we cannot calculate its Cronbach α, and no calculation will be performed for its AVE and CR.

Table 4. Construct reliability and validity for active user.

Construct	Items	Factors Loadings	AVE	CR	Cronbach α
Perceived Privacy Control	PPC01	0.964	0.923	0.960	0.916
	PPC02	0.957			
Perceived Privacy Risk	PPR01	0.600	0.519	0.761	0.598
	PPR02	0.727			
	PPR03	0.818			
Self-Presentation	SP01	0.775	0.676	0.862	0.760
	SP02	0.827			
	SP03	0.861			
Personal Data Security Awareness	PDS02	0.775	0.573	0.838	0.736
	PDS03	0.850			
	PDS05	0.837			
	PDS06	0.516			

As shown in Table 5, hypotheses with a T value above 1.960 highly correlate with, and positively influence, personal data security awareness. According to the calculation, it is proven that perceived privacy control and self-presentation in active users affects the level of personal data security awareness.

Table 5. PLS path coefficients analysis for active user.

Hypotheses	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Value	Support
Perceived Privacy Control → Personal Data Security Awareness	0.491	0.484	0.074	6.654	Yes
Perceived Privacy Risk → Personal Data Security Awareness	0.042	0.067	0.083	0.508	No
Perceived Security → Personal Data Security Awareness	0.030	0.025	0.088	0.343	No
Self-Presentation → Personal Data Security Awareness	0.338	0.346	0.085	3.962	Yes

Figure 2 shows the path analysis result for an active user using SmartPLS.

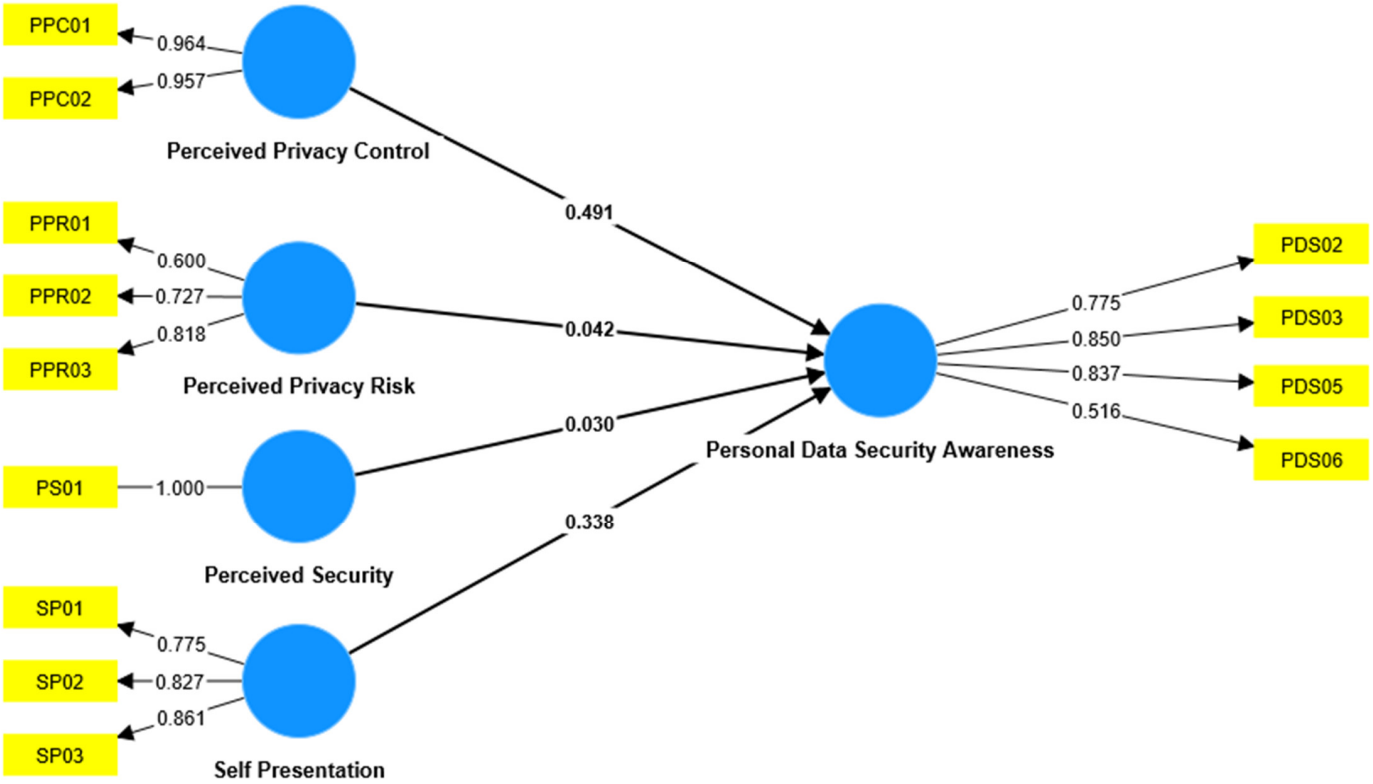

Figure 2. PLS path analysis for active user.

As shown in Table 6, the majority of the Cronbach α values were more than 0.500, following the benchmarked score of 0.500, and these can thus be accepted as reliable [27]. The construct of "Perceived Privacy Control" managed to score more than 0.900, which means that the data collected have high reliability. Since the constructs of "Perceived Security" and "Subjective Norm" are factors with only one single item, we cannot calculate the Cronbach α, and no calculation will be performed for its AVE and CR.

As shown in Table 7, hypotheses with a T value above 1.960 highly correlate with personal data security awareness. According to the calculation, it is proven that perceived privacy control, perceived security and subjective norm in passive users affect the level of personal data security awareness. It is also shown that "Subjective Norm" negatively influences personal data security awareness.

Table 6. Construct reliability and validity for passive user.

Construct	Items	Factors Loadings	AVE	CR	Cronbach α
Perceived Privacy Control	PPC01 PPC02	0.950 0.961	0.914	0.955	0.906
Perceived Privacy Risk	PPR01 PPR02 PPR03	0.838 0.795 0.623	0.574	0.799	0.661
Personal Data Security Awareness	PDS01 PDS02 PDS03 PDS04 PDS05	0.610 0.548 0.833 0.644 0.595	0.427	0.785	0.662

Table 7. PLS path coefficients analysis for passive user.

Hypotheses	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Value	Support
Perceived Privacy Control → Personal Data Security Awareness	0.296	0.299	0.102	2.902	Yes
Perceived Privacy Risk → Personal Data Security Awareness	0.070	0.095	0.111	0.632	No
Perceived Security → Personal Data Security Awareness	0.310	0.310	0.102	3.029	Yes
Subjective Norm → Personal Data Security Awareness	−0.253	−0.253	0.108	2.356	Yes

Figure 3 shows the path analysis result for a passive user using SmartPLS.

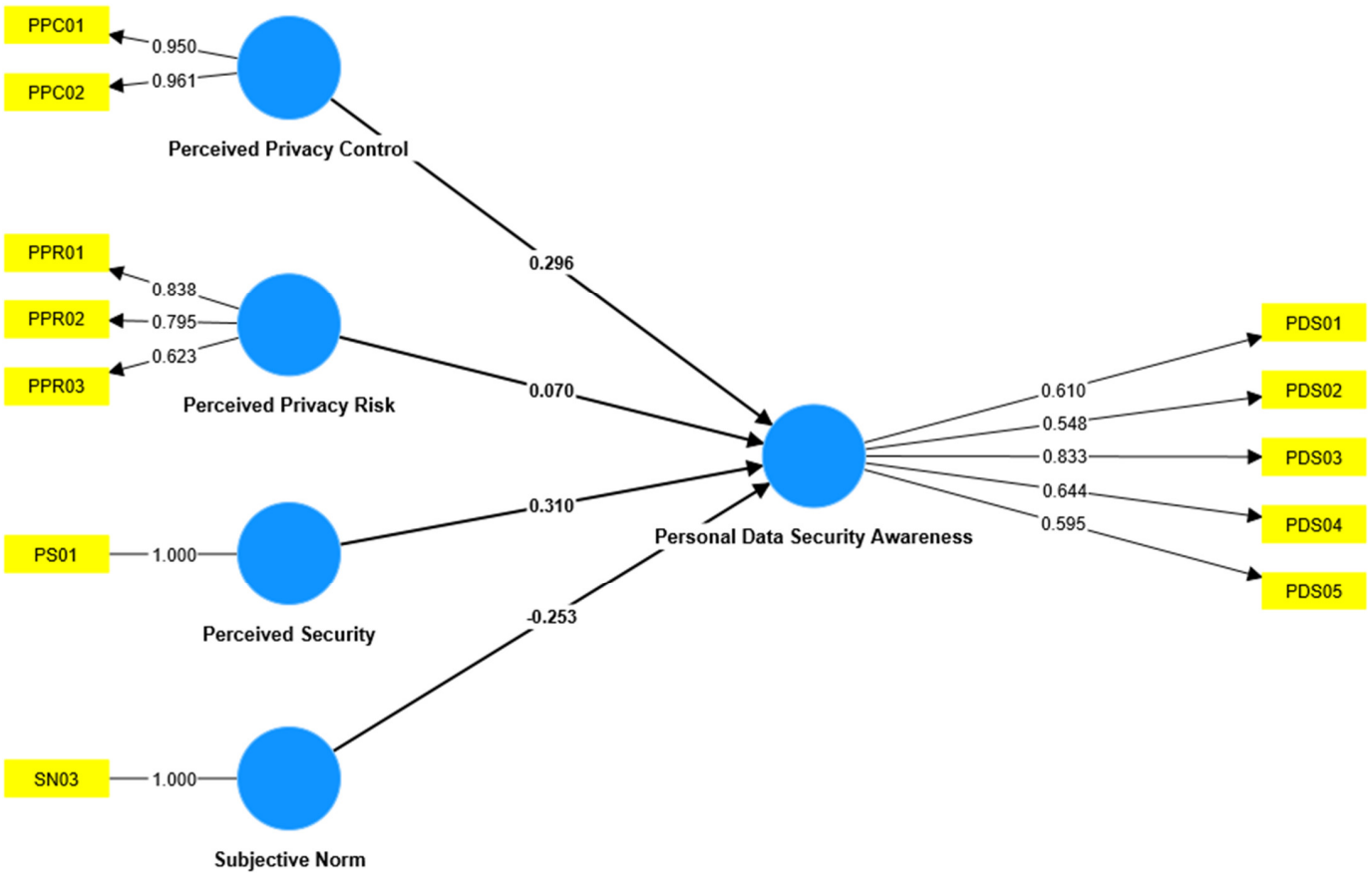

Figure 3. PLS path analysis for passive user.

4.3. Discussions

Based on the results obtained from 204 respondents, active users have a better understanding of the Terms of Service and Privacy Policy. These are the basic requirements when registering for any social media, because they provide guidelines and policies for using it. In addition, there will also be policies regarding the data taken and processed by social media, as well as the purposes of the data collection. As such, social media users should read and fully understand them.

A good password is also required as one of the social media accounts' first forms of security. A good password can be defined as a unique combination consisting of a mixture of numbers, symbols, uppercase letters, and lowercase letters, with a length of at least eight characters. Passwords should be changed frequently, such that passwords are not easily guessed by others and these people do not gain access to your account. Users who are active on social media should be able to implement this because it can protect them while surfing their social media. Passive users are also expected to do the same because someone can guess passwords that are rarely changed as they have easy or common combinations. Accounts that can be guessed will then be used to gain certain benefits from the breachers who do so.

When creating a password, one should avoid combinations made up of consecutive numbers or repeating numbers, or consisting of only numbers, letters, date of birth, names, addresses, and other personal data.

Two-factor authentication is a security measure that every social media user can apply to ensure that someone who logs into a social media account is the account owner. It can be implemented by using an OTP (one-time password). Two-factor authentication will be triggered when a new device tries to access an account in order to help prevent and detect suspicious access.

As regards linked account settings, when creating a social media account, one will usually be given the option to use an existing account or a registered Google account. The Google account that is used to create a social media account will usually be given access to the social media for some data contained in your profile and friends in your Google account network. This condition will certainly pose a risk if your google account stores some personal data.

The use of personal data itself includes creating a social media profile that uses your real personal information, such as your identity card's full name, age, place of birth, and personal photo. Creating a profile with these data will certainly pose a risk because other people can easily imitate you and use the information for bad purposes, such as fraud against your friends or acquaintances. When creating a profile, it is better to disguise or mask part of our data, such as using a pseudonym or short name, fake or anonymous profile pictures, and altered dates of birth and age. Thus, it will be difficult for someone to imitate your social media account and perform fraudulent activities on behalf of your account.

Another form of using personal data is social media content. Some people think that uploading personal data can attract many other users, but remember that it can pose various threats. For example, status updates that include uploading recent activities and locations on the content can attract criminals in the vicinity to approach and attack you. In addition, if you upload personal data too often, even though in a different period, some people will be able to collect them and then make a complete personal profile.

To mitigate the risk of using personal data on social media, we can implement good cyber hygiene; we should start to be more aware of our content, cover or anonymize data that do not need to be shown, and set the privacy settings on social media so that only certain people can see our content.

After scrolling through our social media, it is recommended for us to log out from the account; this is to ensure that when someone tries opens a device that is usually used for our social media, it is difficult for them to access our social media accounts directly, because they need to re-enter the account password.

These things should be done to create a safer social media environment and safeguard our data, because something uploaded on social media will be difficult to delete or change as some other users may have saved it. In brief, the process of how each user uses social media and what factors influence their behavior, coming both from themselves and from social media itself, in maintaining personal data security has been described in Figure 4. The level of awareness may differ between countries in accordance with their target users and advancement of technology. The output of this research is focused on higher education students, since the largest age group in Indonesia that accesses social media is 18–34 [3], which is slightly different from Turkey and Iraq [15], where most of the active social media users are 10–20 years old. In addition, Figure 5 provides an overview of the personal data security awareness of the two users.

The results of the hypothesis test analysis using SmartPLS can be seen in Tables 5 and 7, and the results of path analysis are shown in Figures 2 and 3. Table 5 illustrates the results of hypothesis testing for the type of active social media users with the correct hypothesis or "accepted", such as the relationship between Perceived Privacy Control and Personal Data Security Awareness, or H2. Perceived Privacy Control has a positive relationship with Personal Data Security Awareness; this is proven true because the more aware a person is of the control they have over their data, the more aware they are of disclosing their data to the public. In addition, the relationship between Self-Presentation and Personal Data Security Awareness is proven because Self-Presentation can be said to be a difficult thing to eliminate, especially for social media activists, because they need to upload content even though they must let other users see their data.

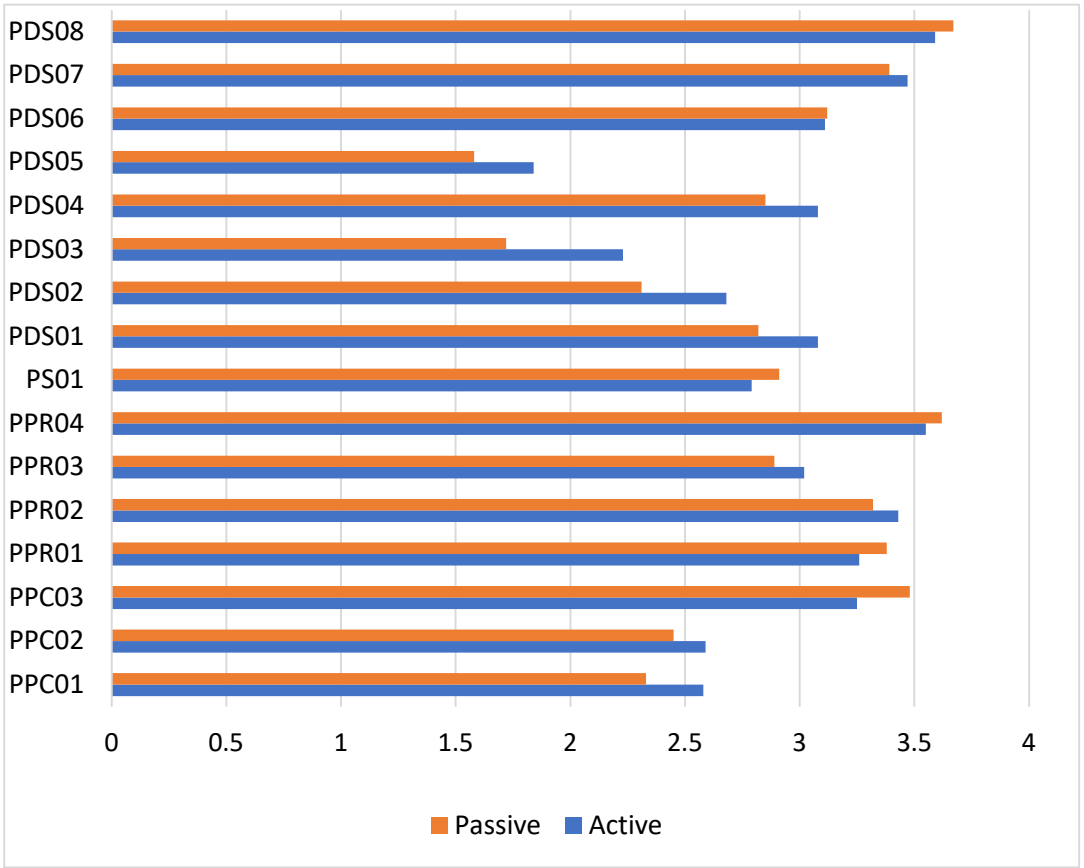

Figure 4. Comparison between active and passive users.

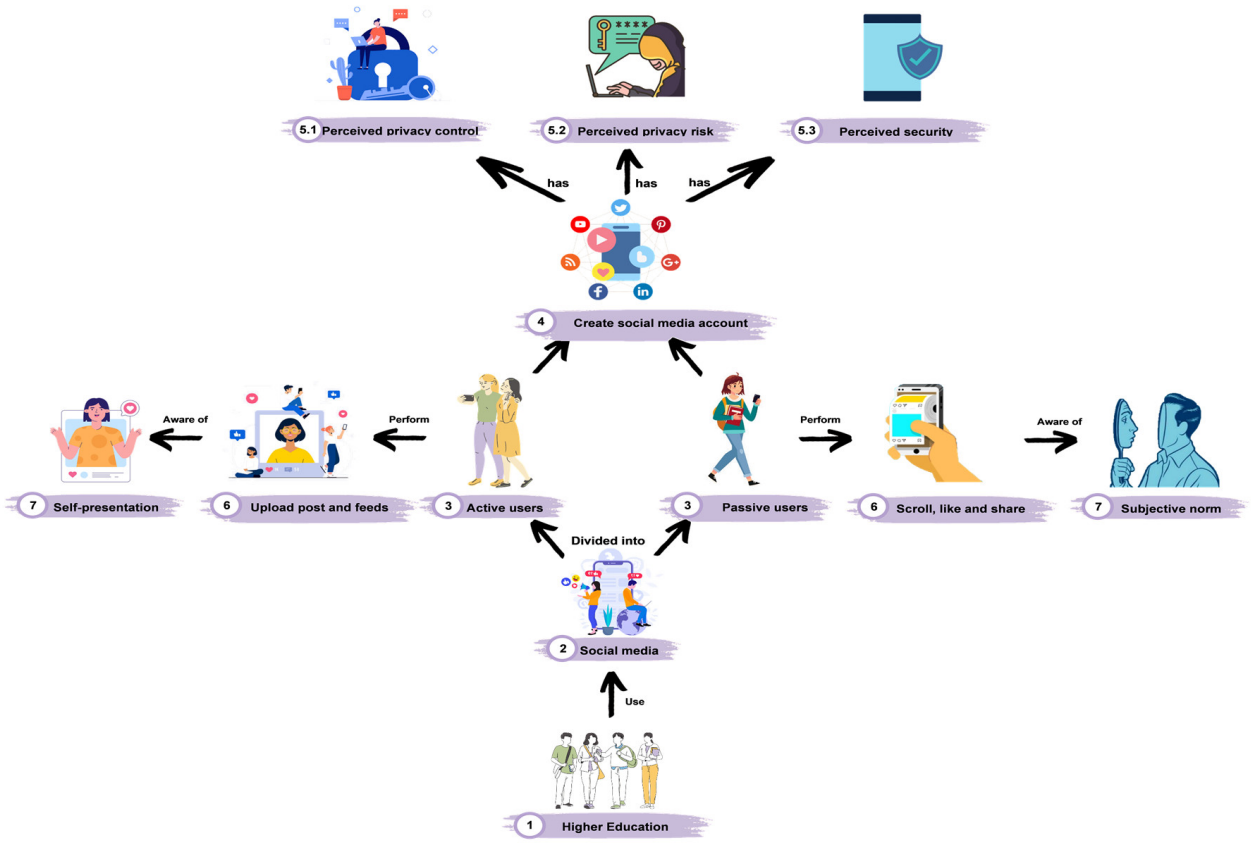

Figure 5. Rich picture about personal data security awareness.

Table 7 illustrates the results of hypothesis testing for passive users of social media. Three hypotheses can be stated as true or accepted. The first hypothesis is the relationship between Perceived Privacy Control and Personal Data Security Awareness regarding the request for full control of data owners over their data, so that they will not upload their data if they do not get this control. The second hypothesis is the relationship between Perceived Security and Personal Data Security Awareness regarding the level of user confidence in the level of security of their social media, so that some users no longer apply several other security measures to their accounts. The third hypothesis is the relationship between Subjective Norms and Personal Data Security Awareness regarding how passive users decide not to upload content to their social media too often, because they think about the judgment that will be held by others [40]; it also influences them not to reveal their data on social media, so that the data cannot be misused by others, and also, they can maintain their image or good name. This study aims to overview higher education students' awareness of personal data security on social media, especially in Indonesia. This study differentiates social media users into two types, active users and passive users, and defines an active user as someone who actively creates content on social media in the form of pictures or videos. In contrast, a passive user rarely uploads content on social media and only uses social media as a means of entertainment. Our study is expected to provide an overview of the current state of social media users in Indonesia for other future research, because research on social media users in Indonesia is relatively lacking, especially regarding awareness of personal data security from the perspective of two different user types, active and passive.

5. Conclusions

The research conducted is limited to the awareness of Indonesia's higher education students, with a total number of 204 respondents. Based on the performed research, it can be concluded that factors affecting the awareness of active and passive users in maintaining their data on social media are quite different and contradictory, because, on the one hand, while some want to look more prominent, on the other hand, they do not want to look too prominent on their social media accounts. From the 204 respondents, it can be concluded that active users have a better awareness of security measures than passive users. This condition is necessary for people who are active on social media because they can avoid any form of cyberattacks. Meanwhile, passive users need to increase their awareness regarding the security of their data and accounts; even though they rarely use social media, a good level of security is needed. The SmartPLS analysis has also proven that five out of the eight hypotheses are valid.

Besides the security factor, social media users are also expected to be more careful in uploading content, because once uploaded, it will be difficult to remove it. In addition, social media users must also be careful in following a trend that takes place on social media. Some people can take advantage of the trend to dig up or get someone's data, and then use it for certain purposes, such as social engineering. Everything related to social media must be read and understood properly, especially regarding the Terms of Service and Privacy Policy of social media. The security features provided must also be applied, changing passwords regularly, logging out after using it, or even not saving log-in information to prevent security risks from occurring, and to create a safe atmosphere or boundaries when using social media.

Author Contributions: Conceptualization, Y.K., S.I.S. and R.R.W.; methodology, Y.K. and S.I.S.; validation, Y.K. and R.R.W.; formal analysis, Y.K. and R.R.W.; investigation, S.I.S. and R.R.W.; resources, S.I.S.; data curation, Y.K., S.I.S. and R.R.W.; writing—original draft preparation, S.I.S.; writing—review and editing, N.A., G.B. and R.R.W.; visualization, R.R.W.; supervision, Y.K. and S.I.S.; project administration, E.H., S.I.S. and R.R.W. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: The study was conducted in accordance with the Declaration of Helsinki, and approved by the Institutional Review Board (or Ethics Committee) of Bina Nusantara University.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: Data used in the study (the survey results) can be found in references.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Table A1. Questionnaire questions.

No.	Statement	Answer (Options)	Reference
		Profiling	
1.	Studies Major	• Accounting • Taxation • Finance • Visual Communication Design • Interior Design • Film • Management • Business • International Business Management • Global Business Marketing • Business Management • Marketing Communication • Mass Communication • Public Relations • Computer • Business Analytics • Data Science • Information Systems Accounting and Auditing • Information Systems • Business Information Technology • Others (Short answer)	
2.	Type of social media users	• Active • Passive	
3.	The most used social media	• Youtube • Whatsapp • Facebook • Instagram • Tiktok • Line • Twitter • Others (Short answer)	

Table A1. *Cont.*

Social Media Active Users			
Perceived Privacy Control			
No.	**Indicators/Statement**	**Answer (Options)**	
PPC01.	I have read and understand the Terms of Service of the social media I use.	1. Strongly Disagree 2. Disagree 3. Agree 4. Strongly Agree	Perceived privacy control is a person's ability to collect, change, and use personal data (O. H. Al-laymoun and A. Aljaafreh, "Examining Users' Willingness to Post Sensitive Personal Data on Social Media", *IJACSA*, 2020) [27].
PPC02.	I read and understand the Privacy Policy of the social media I use.	1. Strongly Disagree 2. Disagree 3. Agree 4. Strongly Agree	
PPC03.	I understand that the flow of data spread on social media cannot be controlled by the owner of the data.	1. Strongly Disagree 2. Disagree 3. Agree 4. Strongly Agree	
Perceived Privacy Risk			
PPR01.	I am aware that my account's data can be used by social media developers/companies.	1. Strongly Disagree 2. Disagree 3. Agree 4. Strongly Agree	Perceived privacy risk is an understanding of each user regarding the privacy risks they can experience while using social media (O. H. Al-laymoun and A. Aljaafreh, "Examining Users' Willingness to Post Sensitive Personal Data on Social Media", *IJACSA*, 2020) [27].
PPR02.	I am aware that if I use another account to register, social media will have access to the linked account data.	1. Strongly Disagree 2. Disagree 3. Agree 4. Strongly Agree	
PPR03.	I am aware that my account data can be accessed and stored by other users.	1. Strongly Disagree 2. Disagree 3. Agree 4. Strongly Agree	
PPR04.	I know of at least one form of personal data attack or threat on social media.	1. Strongly Disagree 2. Disagree 3. Agree 4. Strongly Agree	
Perceived Security			
PS01.	I believe that the social media I use has a good level of security.	1. Strongly Disagree 2. Disagree 3. Agree 4. Strongly Agree	Perceived security is about the level of user trust on the provided or guaranteed social media security (K. Sutarno, B. Estadimas, A. Taliya, D. Wardoyo, I. C. Hapsari and A. N. Hidayanto, "Factors Influencing User Intention in Opening Personal Data on Social Media", 2020) [30].

Table A1. *Cont.*

Self Presentation			
SP01.	I only care about the number of other users who see the content I create.	1. Strongly Disagree 2. Disagree 3. Agree 4. Strongly Agree	Self-presentation can be interpreted as a behavior or action taken by someone, in this context meaning social media users with the aim of adjusting or introducing themselves to the public (K. Sutarno, B. Estadimas, A. Taliya, D. Wardoyo, I. C. Hapsari and A. N. Hidayanto, "Factors Influencing User Intention in Opening Personal Data on Social Media", 2020) [30].
SP02.	I created content without considering the safety of the personal data in it.	1. Strongly Disagree 2. Disagree 3. Agree 4. Strongly Agree	
SP03.	I used personal data in some content created to attract the attention of other users.	1. Strongly Disagree 2. Disagree 3. Agree 4. Strongly Agree	
Personal Data Security Awareness			
PDS01	I use unique and complex password variations.	1. Strongly Disagree 2. Disagree 3. Agree 4. Strongly Agree	Personal data security awareness can be defined as the knowledge of security measures that can be taken to protect personal data on social media. Several things that can affect the level of awareness are age, education level, security training obtained (F. Reer, W. Y. Tang and T. Quandt, "Psychosocial well-being and social media engagement: The mediating roles of social comparison orientation and fear of missing out", *Sage*, 2019) [14]. , the level of psychosocial health of each user, FoMO behavior (A. Sundaram, "Social media security and privacy protection concerning youths. 'How to be safe, secure and social'", 2019) [13], or the level of user trust in social media usually due to perceived enjoyment, benefits obtained, and status (S. S. Sundar and J. Kim, "Machine Heuristic: When We Trust Computers More than Humans with Our Personal Information", *CHI*, 2019) [9].
PDS02	I use a different password for each of the account I have.	1. Strongly Disagree 2. Disagree 3. Agree 4. Strongly Agree	
PDS03	I periodically change my password.	1. Strongly Disagree 2. Disagree 3. Agree 4. Strongly Agree	
PDS04	I use two-factor authentication for every account I have.	1. Strongly Disagree 2. Disagree 3. Agree 4. Strongly Agree	
PDS05	I log-in and log-out every time I use social media.	1. Strongly Disagree 2. Disagree 3. Agree 4. Strongly Agree	
PDS06	I understand and use the security or privacy features provided by social media.	1. Strongly Disagree 2. Disagree 3. Agree 4. Strongly Agree	
PDS07	I never upload or share personal data on social media.	1. Strongly Disagree 2. Disagree 3. Agree 4. Strongly Agree	
PDS08	I am aware that the data that has been spread on social media will be difficult to change and delete.	1. Strongly Disagree 2. Disagree 3. Agree 4. Strongly Agree	

Table A1. *Cont.*

Pengguna Pasif Media Sosial			
Perceived Privacy Control			
No.	**Indicators/Statement**	**Answer (Options)**	
PPC01.	I have read and understand the Terms of Service of the social media I use.	1. Strongly Disagree 2. Disagree 3. Agree 4. Strongly Agree	Perceived privacy control is a person's ability to collect, change, and use personal data (O. H. Al-laymoun and A. Aljaafreh, "Examining Users' Willingness to Post Sensitive Personal Data on Social Media", *IJACSA*, 2020) [27].
PPC02.	I read and understand the Privacy Policy of the social media I use.	1. Strongly Disagree 2. Disagree 3. Agree 4. Strongly Agree	
PPC03.	I understand that the flow of data spread on social media cannot be controlled by the owner of the data.	1. Strongly Disagree 2. Disagree 3. Agree 4. Strongly Agree	
Perceived Privacy Risk			
PPR01.	I am aware that my account's data can be used by social media developers/companies.	1. Strongly Disagree 2. Disagree 3. Agree 4. Strongly Agree	Perceived privacy risk is an understanding of each user regarding the privacy risks they can experience while using social media (O. H. Al-laymoun and A. Aljaafreh, "Examining Users' Willingness to Post Sensitive Personal Data on Social Media", *IJACSA*, 2020) [27].
PPR02.	I am aware that if I use another account to register, social media will have access to the linked account data.	1. Strongly Disagree 2. Disagree 3. Agree 4. Strongly Agree	
PPR03.	I am aware that my account data can be accessed and stored by other users.	1. Strongly Disagree 2. Disagree 3. Agree 4. Strongly Agree	
PPR04.	I know of at least one form of personal data attack or threat on social media.	1. Strongly Disagree 2. Disagree 3. Agree 4. Strongly Agree	
Perceived Security			
PS01.	I believe that the social media I use has a good level of security.	1. Strongly Disagree 2. Disagree 3. Agree 4. Strongly Agree	Perceived security is about the level of user trust on the provided or guaranteed social media security (K. Sutarno, B. Estadimas, A. Taliya, D. Wardoyo, I. C. Hapsari and A. N. Hidayanto, "Factors Influencing User Intention in Opening Personal Data on Social Media", 2020) [30].

Table A1. *Cont.*

Subjective Norm			
SN01.	I don't like being the center of attention or a star on social media.	1. Strongly Disagree 2. Disagree 3. Agree 4. Strongly Agree	Subjective norm is about a person's behavior in taking an action by considering things that may judge him usually the judgement can come from the people closest to him (A. B. Cengiz, G. Kalem and P. S. Boluk, "The Effect of Social Media User Behaviors on Security and Privacy Threats", *IEEE*, 2022) [15], (J. A. Cain, "How Much for My Name? Privacy Perceptions and Motivations for Sharing Personal Information on Social Networking Sites", *JSMS*, 2021) [31].
SN02.	I sometimes upload a few short content that has a certain time span.	1. Strongly Disagree 2. Disagree 3. Agree 4. Strongly Agree	
SN03.	I consider the judgement of other users when creating a content.	1. Strongly Disagree 2. Disagree 3. Agree 4. Strongly Agree	
Personal Data Security Awarenesss			
PDS01	I use unique and complex password variations.	1. Strongly Disagree 2. Disagree 3. Agree 4. Strongly Agree	Personal data security awareness can be defined as the knowledge of security measures that can be taken to protect personal data on social media. Several things that can affect the level of awareness are age, education level, security training obtained (F. Reer, W. Y. Tang and T. Quandt, "Psychosocial well-being and social media engagement: The mediating roles of social comparison orientation and fear of missing out", *Sage*, 2019) [14] , the level of psychosocial health of each user, FoMO behavior (A. Sundaram, "Social media security and privacy protection concerning youths. 'How to be safe, secure and social'", 2019) [13], or the level of user trust in social media usually due to perceived enjoyment, benefits obtained, and status (S. S. Sundar and J. Kim, "Machine Heuristic: When We Trust Computers More than Humans with Our Personal Information", *CHI*, 2019) [9].
PDS02	I use a different password for each of the account I have.	1. Strongly Disagree 2. Disagree 3. Agree 4. Strongly Agree	
PDS03	I periodically change my password.	1. Strongly Disagree 2. Disagree 3. Agree 4. Strongly Agree	
PDS04	I use two-factor authentication for every account I have.	1. Strongly Disagree 2. Disagree 3. Agree 4. Strongly Agree	
PDS05	I log-in and log-out every time I use social media.	1. Strongly Disagree 2. Disagree 3. Agree 4. Strongly Agree	
PDS06	I understand and use the security or privacy features provided by social media.	1. Strongly Disagree 2. Disagree 3. Agree 4. Strongly Agree	
PDS07	I never upload or share personal data on social media.	1. Strongly Disagree 2. Disagree 3. Agree 4. Strongly Agree	
PDS08	I am aware that the data that has been spread on social media will be difficult to change and delete.	1. Strongly Disagree 2. Disagree 3. Agree 4. Strongly Agree	
Total Questions:		**40**	

References

1. Hootsuite (We Are Social): Indonesian Digital Report 2019. 2019. Available online: https://andi.link/hootsuite-we-are-social-indonesian-digital-report-2019/ (accessed on 29 October 2022).
2. Hootsuite (We Are Social): Indonesian Digital Report 2022. 2022. Available online: https://andi.link/hootsuite-we-are-social-indonesian-digital-report-2022/ (accessed on 29 October 2022).
3. Hasil Survei Profil Internet Indonesia 2022. 2022. Available online: https://apjii.or.id/content/read/39/559/Laporan-Survei-Profil-Internet-Indonesia-2022 (accessed on 29 October 2022).
4. Data Digital Indonesia Tahun 2022. 2022. Available online: https://www.kompasiana.com/andidwiriyanto/620fe14651d76471ad402f76/data-digital-indonesia-tahun-2022?page=1&page_images=1 (accessed on 29 October 2022).
5. Tren Baru Challenge Share Instagram Ternyata Berbahaya Penipuan? Waspada Bagikan Data Pribadi! 2021. Available online: https://kuyou.id/homepage/read/27591/tren-baru-challenge-share-instagram-ternyata-berbahaya-penipuan-waspada-bagikan-data-pribadi (accessed on 29 October 2022).
6. Social Engineering, Ancaman Manipulasi Psikologis di Balik IG Story Add Yours. 2021. Available online: https://kumparan.com/kumparannews/social-engineering-ancaman-manipulasi-psikologis-di-balik-ig-story-add-yours-1wyWX9hcPJR (accessed on 29 October 2022).
7. Ryz, L.; Grest, L.; Ontrack, K. A New Era in Data Protection. *Comput. Fraud Secur.* **2016**, *2016*, 18–20. [CrossRef]
8. Romansky, R. Social Media and Personal Data Protection. *Int. J. Inf. Technol. Secur.* **2014**, *6*, 65–80.
9. Sundar, S.S.; Kim, J. Machine Heuristic: When We Trust Computers More than Humans with Our Personal Information. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, Glasgow, UK, 4–9 May 2019.
10. Lina, X.; Wang, X. Examining gender differences in people's information-sharing decisions on social networking sites. *Int. J. Inf. Manag.* **2020**, *50*, 45–56. [CrossRef]
11. Pianese, T.; Belfiore, P. Exploring the Social Networks' Use in the Health-Care Industry: A Multi-Level Analysis. *Int. J. Environ. Res. Public Health* **2021**, *18*, 7295. [CrossRef] [PubMed]
12. Mahmoodi, J.; Curdova, J.; Henking, C.; Kunz, M.; Matic', K.; Mohr, P.; Vovko, M. Internet Users' Valuation of Enhanced Data Protection on Social Media: Which Aspects of Privacy Are Worth the Most? *Front. Psychol.* **2018**, *9*, 1516. [CrossRef] [PubMed]
13. Sundaram, A. Social media security and privacy protection concerning youths. 'How to be safe, secure and social'. *Int. J. Bus. Innov. Res.* **2019**, *18*, 453–471. [CrossRef]
14. Reer, F.; Tang, W.Y.; Quandt, T. Psychosocial well-being and social media engagement: The mediating roles of social comparison orientation and fear of missing out. *New Media Soc.* **2019**, *21*, 1486–1505. [CrossRef]
15. Cengiz, A.B.; Kalem, G.; Boluk, P.S. The Effect of Social Media User Behaviors on Security and Privacy Threats. *IEEE Access* **2022**, *10*, 57674–57684. [CrossRef]
16. Rodgers, N.S. Understanding Personal Data in the World of Social Media. Undergraduate Honors. Program Thesis, Utah State University, Logan, UT, USA, 2020.
17. General Data Protection Regulation. GDPR.eu. 2016. Available online: https://www.gdpreu.org/the-regulation/key-concepts/personal-data/ (accessed on 8 November 2022).
18. Borzykh, P. Concept of Personal Data in Social Media Environment: Effect of General Data Protection Regulation and Trade Secrets Directive. 2022. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4105982 (accessed on 8 November 2022).
19. Tskhovrebashvili, N. Economic and Social Exchange of Personal Data and the Risks of Their Protection. *Vectors Soc. Sci.* **2021**, *1*, 53–68. [CrossRef]
20. National Institue of Standards and Technology. nist.gov. US Government. Available online: https://csrc.nist.gov/glossary/term/infosec (accessed on 8 November 2022).
21. Kosznik-Biernack, S. The Analysis of Risks to Personal Data Security. *Secur. Dimens.* **2020**, *34*, 256–267. [CrossRef]
22. ISO. 2022. Available online: https://www.iso.org/isoiec-27001-information-security.html (accessed on 8 November 2022).
23. ISACA. isaca.org. 2019. Available online: https://www.isaca.org/resources/cobit#:~:text=COBIT%202019%20is%20a%20framework,that%20supports%20enterprise%20goal%20achievement (accessed on 8 November 2022).
24. Hasanah, M. Viva Tekno. *Viva News*. 21 September 2022. Available online: https://www.viva.co.id/digital/digilife/1523677-membandingkan-sanksi-pada-uu-pdp-dan-gdpr-uni-eropa#:~:text=Dalam%20pembuatannya%20regulasi%20ini%20mengacu%20pada%20General%20Data,landasan%20hukum%20terkait%20perlindungan%20data%20pribadi%20di%20Indonesia (accessed on 8 November 2022).
25. González-Padilla, D.A.; Tortolero-Blanco, L. Social media influence in the COVID-19 Pandemic. *Int. Braz. J. Urol.* **2020**, *46*, 120–124. [CrossRef]
26. Vițelar, A. Like Me: Generation Z and the Use of Social Media for Personal Branding. *Manag. Dyn. Knowl. Econ.* **2019**, *7*, 257–268. [CrossRef]
27. Al-laymoun, O.H.; Aljaafreh, A. Examining Users' Willingness to Post Sensitive Personal Data on Social Media. *Int. J. Adv. Comput. Sci. Appl.* **2020**, *11*, 451–458. [CrossRef]
28. Li, Y.; Xie, Y. Is a Picture Worth a Thousand Words? An Empirical Study of Image Content and Social Media Engagement. *J. Mark. Res.* **2019**, *57*, 1–19. [CrossRef]
29. Oliveira, T.; Araujo, B.; Tam, C. Why do people share their travel experiences on social media? *Tour. Manag.* **2020**, *78*, 104041. [CrossRef]

30. Sutarno, K.; Estadimas, B.; Taliya, A.; Wardoyo, D.; Hapsari, I.C.; Hidayanto, A.N. Factors Influencing User Intention in Opening Personal Data on Social Media. In Proceedings of the 2020 Fifth International Conference on Informatics and Computing (ICIC), Gorontalo, Indonesia, 3–4 November 2020.
31. Cain, J.A. How Much for My Name? Privacy Perceptions and Motivations for Sharing Personal Information on Social Networking Sites. *J. Soc. Media Soc.* **2021**, *10*, 140–161.
32. Soomro, T.R.; Hussain, M. Social Media-Related Cybercrimes and Techniques for Their Prevention. *Appl. Comput. Syst.* **2019**, *24*, 9–17. [CrossRef]
33. Kröger, J.L.; Miceli, M.; Müller, F. How Data Can Be Used Against People: A Classification of Personal Data Misuses. 2021. Available online: https://ssrn.com/abstract=3887097 (accessed on 8 November 2022).
34. Pendergrast, T.R.; Jain, S.; Trueger, N.S.; Gottlieb, M.; Woitowich, N.C.; Arora, V.M. Prevalence of Personal Attacks and Sexual Harassment of Physicians on Social Media. *JAMA Intern. Med.* **2021**, *181*, 550–552. [CrossRef]
35. Koyuncu, M.; Pusatli, T. Security Awareness Level of Smartphone Users: An Exploratory Case Study. *Mob. Inf. Syst.* **2019**, *2019*, 2786913. [CrossRef]
36. Padmavathi, D.J.; Mohanlal, S.A.K. A Study on Extent of Awareness Among College Students in Security and Privacy Issues in Social Media. *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.* **2021**, *7*, 676–682. [CrossRef]
37. Alqahtani, M.A. Factors Affecting Cybersecurity Awareness among University Students. *Appl. Sci.* **2022**, *12*, 2589. [CrossRef]
38. Amin, M.; Tasmil; Herman; Bahrawi; Alam, N.; Dhahir, D.F.; Hadiyat, Y.D. Security and privacy awareness of smartphone users in Indonesia. *J. Phys. Conf. Ser.* **2021**, *1882*, 012134. [CrossRef]
39. Verduyn, P.; Gugushvili, N.; Massar, K.; Täht, K.; Kross, E. Social comparison on social networking sites. *Curr. Opin. Psychol.* **2020**, *36*, 32–37. [CrossRef] [PubMed]
40. Duffy, B.E.; Chan, N.K. "You never really know who's looking": Imagined surveillance across social media platforms. *New Media Soc.* **2019**, *21*, 119–138. [CrossRef]