Journal of
Information Systems Engineering
and Business Intelligence

Vol.6, No.2, October 2020
Available online at: http://e-journal.unair.ac.id/index.php/JISEBI

Information Privacy Concerns Among Instagram Users: The Case of Indonesian College Students

Eko Wahyu Tyas Darmaningrat[1)*], Hanim Maria Astuti[2)], Fadhila Alfi[3)]

[1)2)3)] *Department of Information Systems, Institut Teknologi Sepuluh Nopember, Indonesia*
Jl. Raya ITS, Kampus ITS Keputih, Sukolilo, Surabaya
[1)] tyas@is.its.ac.id, [2)] hanim@is.its.ac.id, [3)] 5215100092@mahasiswa.integra.its.ac.id

Article history:

Received 18 September 2020
Revised 16 October 2020
Accepted 21 October 2020
Available online 28 October 2020

Keywords:

Behavioral intention
Information privacy concern
IUIPC
Instagram
Risk beliefs
Trusting beliefs

Abstract

Background: Teenagers in Indonesia have an open nature and satisfy their desire to exist by uploading photos or videos and writing posts on Instagram. The habit of uploading photos, videos, or writings containing their personal information can be dangerous and potentially cause user privacy problems. Several criminal cases caused by information misuse have occurred in Indonesia.
Objective: This paper investigates information privacy concerns among Instagram users in Indonesia, more specifically amongst college students, the largest user group of Instagram in Indonesia.
Methods: This study referred to the Internet Users' Information Privacy Concerns (IUIPC) method by collecting data through the distribution of online questionnaires and analyzed the data by using Structural Equation Modelling (SEM).
Results: The research finding showed that even though students are mindful of the potential danger of information misuse in Instagram, it does not affect their intention to use Instagram. Other factors that influence Indonesian college students' trust are Instagram's reputation, the number of users who use Instagram, the ease of using Instagram, the skills and knowledge of Indonesian students about Instagram, and the privacy settings that Instagram has.
Conclusion: The awareness and concern of Indonesian college students for information privacy will significantly influence the increased risk awareness of information privacy. However, the increase in risk awareness does not directly affect Indonesian college students' behavior to post their private information on Instagram.

I. INTRODUCTION

The internet, mobile phones, and social media facilitate sharing and distributing private information online and are an indispensable part of teenagers' daily lives and interactions nowadays. The recent survey results in October 2019 indicate that Indonesia was ranked in the fourth position with more than 60 million Instagram users, behind United States, India, and Brazil [1]. This number is accounted for 22.8% of the entire Indonesian population. Besides, people between 18 to 24 years old age group were the largest user group of Instagram in Indonesia [2]. The popularity of Instagram among Indonesian teenagers motivates many researchers to study the privacy concerns of Instagram users.

Privacy is a critical social issue that influences all people, as privacy concerns prevent people from disclosing themselves in social interactions [3]. There are several online behaviors, such as posting personal activities and interacting with unfamiliar persons, which are risky due to their possibility of causing unpleasant experiences, such as cyberbullying and sexual abuse [4]. The potential profitable and non-profitable utility of personal information that is disseminated online has increased various anxieties about information privacy and data protection. The previous studies advised that users, particularly teenagers, have a lack interest in their online confidentiality because of insufficient awareness of technological advancement and data mining practices [5], and lack of legal protections understanding [6]. Another study suggested that teenagers are concerned about their online confidentiality and mindful of accompanying dangers, but regularly share private information in their online activities [7].

* Corresponding author

ISSN 2443-2555 (online) 2598-6333 (print)
doi: http://dx.doi.org/10.20473/jisebi.6.2.159-168

This research investigates the information privacy concerns among Instagram users in Indonesia, more specifically amongst college students, the largest user group of Instagram in Indonesia. Internet Users' Information Privacy Concerns (IUIPC) model is used to observe the influence of information privacy concerns on trusting beliefs, risk beliefs, and behavioral intention [8]. Data are collected over an online questionnaire and examined using Structural Equation Modelling (SEM) to test the hypotheses.

II. Related Works

Internet Users' Information Privacy Concerns (IUIPC) is a model to describe internet users' concern for personal information confidentiality. The IUIPC model was a development of the Concerns for Information Privacy (CFIP) model [9], which is intended to capture people's attention about organizational information confidentiality practices. Based on the social contract (SC) theory that studied individual insights of fairness and justice, Malhotra et al. advised that online users' concerns are based on three main dimensions, namely collection, control, and awareness of privacy implementation. The IUIPC model is then constructed by relating these three dimensions as specific factors with the concept of trust, namely trusting beliefs, risk beliefs, and behavioral intention [8].

Once employed to information privacy, SC theory recommends that collecting personal information from social media provider platforms should give users control over that information and inform users about the company's planned use of the collected data to be considered fair. Consequently, Malhotra et al. conceptualize IUIPC as the concern of Internet users toward the collection of personal information through social media, the users' control of the information that has been collected, and the users' awareness of how the collected information is managed.

Sipior et al. reevaluated the IUIPC construct and hypotheses to assess this construct's continued applicability [10], as shown in Fig. 1. Consistent with the previous studies by Malhotra [8], the more trust users have for an online platform, the less likely that user is to perceive giving private information as dangerous (H3). Another conformable finding is that the more trust users have for an online platform, the more likely they are to intend to give private information online (H4). Lastly, the more risk users have for giving private information, the less eager they are to disclose such information online (H5). Nevertheless, the outcomes did not hold a negative correlation among the IUIPC theory and user trust in an online platform (H1) and a positive correlation among IUIPC and user risk in giving private information to an online platform (H2).

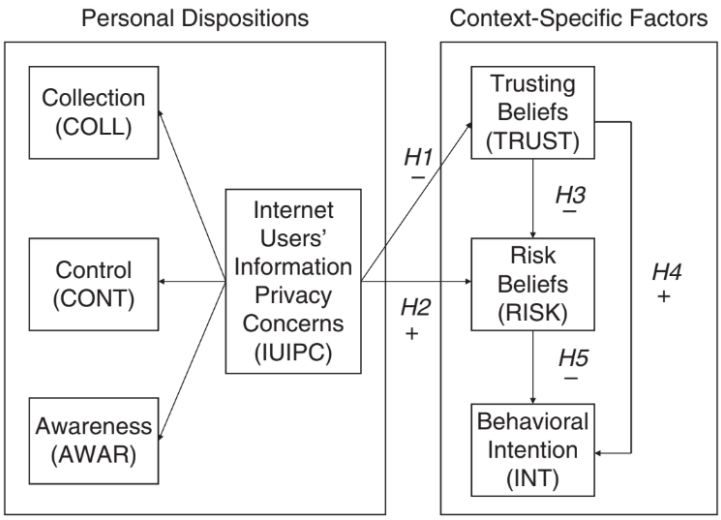

Fig. 1 IUIPC Model - Revisited [10]

Additionally, a recent study by Kusyanti et al. examined Facebook users' apprehensions for information privacy using Internet Users' Information Privacy Concerns (IUIPC) [11]. Alike the previous study by Sipior et al. [10], not all hypotheses were consistent with the result of Malhotra et al. [8]. This research found that IUIPC has a positive consequence on risk beliefs (H2), trusting beliefs have a negative consequence on risk beliefs (H3), and trusting beliefs have a positive consequence on the intention to give private information (H4). Nevertheless, the other two hypotheses were not agreed with the results of Malhotra et al. [8]. The results indicate that IUIPC does not negatively affect trusting beliefs (H1), and risk beliefs do not have a negative consequence on the intention to provide private

information (H5). The authors conclude that although users are aware of possible misuse of information on Facebook, it does not affect their intention to use Facebook.

III. METHODS

A. Conceptual Model and Hypotheses

In this research, the conceptual model and hypotheses referred to the revisited IUIPC model in Fig. 1. This research did not use the contextual variable, namely, type of information since we focus on the user's personal information in social media. Malhotra et al. include the contextual variable by considering that a seller's demand for private information will cause a customer doubtful, subsequently diminishing consumer trust. Based on the model previously explained in Fig. 1, the description of each variable used in this study is explained in Table 1.

TABLE 1
DEFINITION OF EACH VARIABLE

Dimensions	Variables	Definition
Personal Dispositions	Collection	The degree to which an Instagram user is concerned about Instagram's collection of private information.
	Control	The user's control over the collected information (the personal information shared on Instagram).
	Awareness	The user's awareness of how Instagram uses the collected information.
Context-Specific Factors	Trusting Beliefs	The degree of trust that Instagram will protect the user's personal information.
	Risk Beliefs	The degree of awareness in the possible risk of personal information misuse on Instagram.
	Behavioral Intention	User's intention to post personal information on Instagram.

Agreeing with previous studies by Malhotra et al. [8] and Sipior et al. [10], we have the following hypotheses:
H1: IUIPC will have a negative impact on trusting beliefs.
H2: IUIPC will have a positive impact on risk beliefs.
H3: Trusting beliefs will have a negative impact on risk beliefs.
H4: Trusting beliefs have a positive impact on behavioral intention to give personal information on Instagram.
H5: Risk beliefs will have a negative impact on behavioral intention to give personal information on Instagram.

B. Questionnaire Development

The questionnaire was designed based on the adaptation from the result of relevant previous studies. Each variable (as previously explained in Table 1) is decomposed into several indicators used as questionnaire questions. There was a total of 31 questions measured using a seven-point Likert scale item and two open questions. We use 7-point Likert items because it has been demonstrated to deliver a more precise measure of a respondent's true assessment and are more suitable for online questionnaires [12]. The 7-point Likert scale provides different response choices related to an agreement that would be different enough for the participants to respond with no confusion. The questionnaire's open questions are intended to find out what Instagram users have done to protect their personal information on Instagram to avoid information misuse and learn what they need to improve their information privacy awareness on social media.

A pilot study was carried out by conducting face-to-face interviews with five non-IT students to test their understanding and obtain feedback on the questionnaire statements. Although none of the questionnaire's statements are very specific to IT students, we wanted to make sure that the questionnaire statements were easy to understand for students from various departments. In this study, the pilot study was conducted three times by distributing online questionnaires using Google form. In the first pilot study, 30 respondents were participating. The result indicates that 2 item questions are not reliable. Whereas in the second pilot study, the number of respondents was 57 people. The result shows that one question item is invalid. Based on the results of both pilot studies, modifications were made to the questionnaire questions. Furthermore, respondents in the third pilot study were 121 people in total, and the result indicates that all question items are valid and reliable. The questionnaire was then distributed online via social media Twitter by asking help to someone who has many followers to retweet the questionnaire link. A total of 545 respondents filled out the final questionnaire.

C. Measurement Model

To refrain from a misinterpretation of the structural relationships, we approximate a measurement model prior to testing the hypotheses. We followed the two-step approach in which initially, a valid and reliable measurement was established, and afterward, the structural model of Fig. 1 was verified [8]. The questionnaire was tested for data quality, whether the data could meet SEM assumptions or not. Data quality testing comprised of several stages:

1) *Convergent Validity*
   Convergent validity is measured by determining whether each indicator item that is estimated to be valid measures the proposed model's dimensions. Convergent validity is measured by calculating the average variance extracted (AVE) value. If the AVE value is greater than 0.50 or more (ideally greater than 0.70), it can be said that the indicator is valid [13].
2) *Discriminant Validity*
   Discriminant validity is carried out to test whether two or more variables are unique. Discriminant validity of exogenous constructs and endogenous constructs is done separately [14]. A discriminant validity test can be done by testing the correlation number of two constructs. Independent variables must not have a relationship, or the correlation between the two variables must be small or insignificant.
3) *Variable reliability*
   Variable reliability was assessed by calculating the reliability index of the instruments used from the model [13]. The threshold value used to assess a satisfactory level of reliability is > 0.70. However, a value below 0.70 is still acceptable if it is supplemented by empirical reasons seen in the exploratory process. Reliability between 0.5 - 0.6 is also acceptable.
4) *Goodness of Fit (GFI)*
   The Goodness of Fit (GFI) criteria is an evaluation of the feasibility test of a model with several criteria for suitability of the index and its cut-off value to state whether a model can be accepted or rejected [14]. GFI is obtained by measuring the relative number of variants and covariates whose magnitudes range from 0-1. If the value is close to 0, then the model has a low match, and if the value is close to 1, then the model has a good match. There are several criteria to declare a model is fit, first with the Comparative Fit Index (CFI) with a value between 0-1 where if the value approaches the number 1, then the model has a high match, whereas if the value is close to 0, then the model has a low match or not good. Then the Root Mean Square Error of Approximation (RMSEA) serves to consider errors approaching the population. A good model will have a value less than or equal to 0.05 [14].

IV. RESULTS

This research's respondents are students of Institut Teknologi Sepuluh Nopember (ITS, in English: Tenth of November Institute of Technology) from various majors. Online and offline questionnaires were distributed to ITS students with an age range of 18-24 years. Data collection was carried out within two weeks from the end of April 2019 until early May 2019.

A. Descriptive Analysis

The validity test is used to know the extent to which the scores from a measure (i.e., the question items) represent the variable they are intended to. The validity is measured by comparing the Pearson correlation and r-table values. If the p-value is less than 0.05, and the Pearson correlation value is greater than the r-table value, then the question item is proclaimed as valid. The results of the validity test indicated that the entire question items are valid. Besides, reliability tests are being conducted to ascertain the consistency of a measure. The reliability is measured using Cronbach's alpha value on each variable. A variable is reliable if it has a Cronbach's alpha value of more than 0.6. The reliability test results of each variable are shown in Table 2.

There is a total of 545 questionnaire responses with a response rate of 88.8%. Moreover, 484 responses which have passed the consistency test in answering negation questions are used for further analysis. The gender distribution of respondents is relatively balanced, with approximately 65% of respondents aged between 19 to 21 years old. The number of respondents who have been using Instagram for 4 to 5 years is around 25%. In comparison, the number of respondents using Instagram for 2 to 3 hours a day is approximately 40%. Details information of the respondent's characteristics is shown in Table 3.

TABLE 2
RELIABILITY TEST

Variable	Cronbach's α Criteria α > 0,6
Collection	0.604
Control	0.601
Awareness	0.680
Trusting beliefs	0.766
Risk beliefs	0.780
Behavioral intention	0.662

TABLE 3
CHARACTERISTICS OF RESPONDENTS

Profile	Item	Frequency	Percentage
Gender	Male	227	47%
	Female	257	53%
Age	17-18	40	8%
	19-21	316	65%
	22-24	128	26%
Experience in using Instagram	< 1 year	13	3%
	1-2 years	28	6%
	3-4 years	102	21%
	4-5 years	121	25%
	5-6 years	75	15%
	6-7 years	64	13%
	> 7 years	24	5%
Duration in using Instagram	< 1 hour	147	30%
	2-3 hours	195	40%
	4-5 hours	87	18%
	5-6 hours	29	6%
	6-7 hours	14	3%
	> 7 hours	12	2%
Honesty in providing information on Instagram	100%	312	64%
	75%	123	20%
	50%	31	6%
	25%	17	4%
	0%	1	0%
Frequency of being a victim of information misused	Very infrequent	250	52%
	Infrequent	132	27%
	Almost infrequent	81	17%
	Frequent	17	4%
	Very frequent	4	1%
Frequency of knowing about information misused	Not at all	9	2%
	Very rare	28	6%
	Rare	93	19%
	Often	251	52%
	Very often	103	21%

B. Normality Test

SEM analysis requires the normal distribution of variables as one of the assumptions of the maximum likelihood (ML) estimation method [15]. To determine whether the data are normally distributed, it is necessary to test the normality by observing the skewness value and kurtosis. The statistical value to test the normality is called the *Z-value*, which is obtained by using formula (1):

$$Z_{value} = \frac{Skewness}{\sqrt{\frac{6}{N}}}, \text{ N is total population} \quad (1)$$

If Z_{value} is greater than the critical value (Z_{table}), then the data distribution is not normal. Z_{table} is determined based on the significance level of 0.01 (1%); therefore the Z_{table} value will be ± 2.58. Subsequently, the assumption of multivariate normality is observed by looking at the value of critical ration (c.r.), which is obtained from formula (2). If c.r. value is greater than Z_{table}; then the data distribution is considered abnormal. The results of the normality test are shown in Table 4.

$$critical\ ration = \frac{kurtosis\ coefficient}{standard\ error} \quad (2)$$

TABLE 4
NORMALITY TEST

Variable	Z-value	c.r. value	Z-table	Remarks
Collection (CL)	-2.42	-1.06	±2.58	Normal Distribution
Control (CT)	-2.02	-2	±2.58	Normal Distribution
Awareness (AW)	-1.77	-1.08	±2.58	Normal Distribution
Trusting beliefs (TB)	-0.29	-2.18	±2.58	Normal Distribution
Risk beliefs (RB)	-0.88	1.18	±2.58	Normal Distribution
Behavioral Intention (BI)	2.31	-0.62	±2.58	Normal Distribution

C. Measurement Model

The SEM measurement model was assessed based on three tests: convergent validity, discriminant validity, and reliability [13]. The indicators in a model must be convergent or share in a high proportion of variance. Convergent validity is obtained by observing the loading factor values on each indicator. If the loading factor value is greater than 0.70, it is considered to have very good validity. Besides, the loading factor value from 0.50 to 0.60 is still considered good and acceptable. The conclusion of convergent validity on variables can be done by calculating the value of variance extracted (AVE) between variables. If the AVE value is greater than 0.5, then the variable could have good convergent validity. The results of the convergent validity test are described in Table 5.

TABLE 5
CONVERGENT VALIDITY OF EACH VARIABLE

Variable	AVE value	$\sqrt{AVE}$ value	Remarks
Collection (CL)	0.615	0.785	Good
Control (CT)	0.568	0.753	Good
Awareness (AW)	0.54	0.735	Good
Trusting beliefs (TB)	0.504	0.71	Good
Risk beliefs (RB)	0.529	0.727	Good
Behavioral Intention (BI)	0.501	0.708	Good

Discriminant validity measures to what extent a variable is entirely different from other variables [15]. A high discriminant value indicates that a variable is unique and well-captured the phenomenon being measured. The measurement of discriminant validity is conducted by comparing the value of AVE square root ($\sqrt{AVE}$) with the correlation value between variables [13]. The results of the discriminant validity test are as shown in Table 6. The correlation value of all variable with itself is greater than the correlation value between the variable with other variables, which indicate that all variables have good discriminant validity.

TABLE 6
CORRELATION VALUE BETWEEN CONSTRUCTS

	CL	CT	AW	TB	RB	BI
CL	**0.785**					
CT	0.275	**0.753**				
AW	0.141	0.284	**0.735**			
TB	0.094	0.082	0.125	**0.71**		
RB	0.096	0.183	0.090	0.006	**0.727**	
BI	-0.084	-0.047	-0.001	0.195	-0.012	**0.708**

The composite reliability test is a test to determine whether the data processed has a high level of reliability or not [13]. The expected composite reliability (CR) value on each variable is greater than 0.70, while the CR value between 0.60-0.70 is still acceptable with the condition that the indicator validity is stated as good [26]. Variable Collection,

Control, Awareness, Trusting Beliefs, and Risk Beliefs can be declared reliable with a CR value of 0.70. While the Behavioral Intention variable can be declared reliable with a CR value of 0.60 to 0.70 because the variable gets a good convergent validity test value. Detailed results of the composite reliability test are shown in Table 7.

TABLE 7
COMPOSITE RELIABILITY TEST RESULT

Variable	CR value	Remarks
Collection (CL)	0.762	Reliable
Control (CT)	0.724	Reliable
Awareness (AW)	0.701	Reliable
Trusting beliefs (TB)	0.742	Reliable
Risk beliefs (RB)	0.763	Reliable
Behavioral Intention (BI)	0.660	Reliable

D. Goodness of Fit

The goodness of fit measures how well the model is used in research. The goodness of fit test results that have been carried out will be compared with predetermined values. The goodness of fit test carried out on the proposed model indicates that the model has met the criteria of an excellent fit, as shown in Table 8.

TABLE 8
GOODNESS OF FIT

Fit Index	Criteria	Value	Remarks
Chi-Square	Small	79.150	Excellent Fit
P-value	≥ 0.05	0.189	Excellent Fit
CMIN/DF	≤ 2	1.147	Excellent Fit
RMSEA	≤ 0.08	0.017	Excellent Fit
GFI	≥ 0.90	0.977	Excellent Fit
AGFI	≥ 0.90	0.966	Excellent Fit
TLI	≥ 0.90	0.991	Excellent Fit
CFI	≥ 0.95	0.993	Excellent Fit

E. Hypotheses Testing

Path analysis focuses on the estimated value in Standardized Regression Weights to determine the variables' positive or negative relationship. The p-value and CR on the Regression Weights are used to determine the significant level between the two variables. If the estimated value is positive then the two variables have a positive relationship; conversely, if the estimated value is negative then the two variables have a negative relationship. To test the significant relationship between two variables, the CR value must be more than 1.96, and the p-value is less than 0.05; conversely, if the p-value is more than 0.05 and the CR value is less than 1.96, then both variables do not have a significant relationship. Details of the hypotheses test results are shown in Table 9.

H1 (IUIPC will have a negative impact on trusting beliefs) is rejected. The results indicated that concern for student privacy had a positive and significant effect on student trust in sharing personal information on Instagram. Students tend to ignore their concerns when they have a trust that Instagram will not abuse their personal information. This hypothesis's results are consistent with a study conducted by Kuo and Talley [16], who found that users tend to ignore information privacy concerns when they have the confidence and trust that Instagram will not misuse their personal information. Users believe that the application has complied with concerning laws and regulations to maintain the users' information privacy.

H2 (IUIPC will have a positive impact on risk beliefs) is accepted. The results informed that privacy concerns had a positive and significant effect on student awareness of Instagram's risks. Respondents argued that they always think twice about sharing personal information on Instagram, knowing which information should be shared or not, the importance of privacy settings, policies, and handling privacy violations that Instagram must-have, and the importance to be aware of the impact of sharing personal information on Instagram. Besides, respondents also felt worried about something unpleasant that could happen in sharing personal information on Instagram. A study conducted by Öhman (2017) proved that someone's experience of risk could improve their risk beliefs [17]. Thus, someone who has experienced information privacy abuse will have a higher risk of confidence in Instagram. This result is consistent with another research conducted by Dinev and Hart (2004), suggesting that the perception of vulnerability affects the increasing concern for the privacy of someone's privacy concerns. Individuals who experience positive things from

sharing information on Instagram, such as getting a job offer, will argue that sharing information on Instagram does not cause information privacy issues. The perception of vulnerability can vary depending on one's experience [18].

TABLE 9
HYPOTHESES TESTING RESULTS

Hypotheses	Relationship	t-value	p-value	Estimate
			< 0.05*	
Criteria		> 1.96	< 0.01**	
			< 0.001***	
H1	TR ← IUIPC	2.113	0.035	0.175
H2	RS ← IUIPC	3.273	0.001	0.265
H3	RS ← TR	-0.685	0.493	-0.039
H4	BI ← TR	2.069	0.039	0.184
H5	BI ← RS	-0.318	0.751	-0.018

H3 (Trusting beliefs will have a negative impact on risk beliefs) is rejected. The results showed that students' trust in sharing personal information on Instagram negatively affected student awareness of the risks on Instagram. The hypothesis is supported by research conducted by Kuo and Talley [16] and Kusyanti, et al. [11] which mentioned that the more users argue that they have trust in social media, the less confidence the user will have of risk on social media. However, if there is an increase in information privacy concerns on Indonesia's college students, it will not directly impact the reducing level of trust for sharing their personal information on Instagram. Therefore, more effort is needed to influence college students' risk awareness.

H4 (Trusting beliefs have a positive impact on behavioral intention to give personal information on Instagram) is accepted. The results showed that students' trust in sharing personal information on Instagram positively and significantly affected students' intention to post private information on Instagram. Respondents argue that Instagram has privacy settings and policies for the misuse of personal information. Respondents also believe that their followers on Instagram will not misuse their personal information. This is reinforced by the answer to the open question about some actions respondents have done to maintain privacy security by selecting followers and selecting information provided on Instagram, using privacy settings features on Instagram such as Close Friends.

H5 (Risk beliefs will have a negative impact on behavioral intention to give personal information on Instagram) is rejected. The results showed that students' awareness of the risks on Instagram had a negative effect was not significant to the students' intention to share personal information on Instagram. A study proves that the perception of vulnerability influences an increase in privacy concerns for one's personal information. Individuals who experience positive things from sharing information on Instagram, such as getting a job offer, will argue that sharing information on Instagram does not cause information privacy issues. The perception of vulnerability can vary depending on someone's experience [18]. Whereas another research states that decision making is influenced by experience that affects risk preferences [19]. Based on the open question, as many as 79% of respondents have never had a bad experience regarding information privacy. Other factors that can affect one's trust in using internet sites and in providing personal information include being influenced by digital skills [20] [21] [22]. Skills are defined as a person's assessment of his abilities for using the internet site. When users understand that they are able to use an internet site, then one's trust will increase [22]. Then another study found that the greater the user on social media, the greater the person's trust in the people on social media [21] [23]. An internet site's ability to control the information that someone shares and control who can access someone's information can affect one's trust in the internet site [24]. Reputation is also one of the factors that can increase trust. Reputation can be obtained through the vendor or owner of the internet site and also through information from someone who has experience using the internet site (rating) [25]. A person's trust is also influenced by the ease of use of the internet site [26].

V. DISCUSSIONS

One of our research findings indicates that privacy concerns positively and significantly affect students' awareness of Instagram's risks. Therefore, the second hypothesis, which stated that IUIPC would be positively associated with risk beliefs, is accepted. We observed several papers regarding other factors that can influence a person's belief in risk. A study conducted by Ohman [17] proved that a person's experience at risk could increase a person's risk belief perspective. Thus, someone who has experienced information privacy abuse will have a firmer belief in Instagram's risk. This finding is consistent with other research conducted by Dinev and Hart [18], which proves that perceived

vulnerability increases one's privacy concern. Individuals who experience positive things resulting from sharing information on Instagram, such as getting a job offer, will argue that sharing information on Instagram does not raise information privacy issues. Perceptions of vulnerability can vary depending on a person's experience.

In addition, another finding of this research indicates that students' trust in sharing personal information on Instagram is positively and significantly affected students' intention to share personal information on Instagram. Therefore, the fourth hypothesis, which stated that trusting beliefs will be positively associated with behavioral intention to provide personal information on Instagram, is accepted. We compared this finding with several relevant papers regarding other factors that can affect a person's trust in using internet sites and providing personal information. A study proved that a person's trust in social media is influenced by digital skills possessed by a person [20] [21] [22]. Another study found that the greater the number of social media users, the greater their trust in people on social media [20][23]. Someone chooses to use social media to build or maintain social connections. Someone will trust more when a site has information settings for the information that users shared. Reputation is also one of the factors that can increase a person's trust [23]. Reputation can be obtained through the internet site owner or through information from someone who has experience using the internet site [24]. A person's trust is also influenced by the ease of using an internet site [25].

On the other hand, our first hypothesis that IUIPC will be negatively associated with trusting beliefs is rejected. This result is in line with research conducted by Kuang-Ming Kuo et al. [15], which argued that users tend to ignore the awareness of information privacy when they believe that Instagram will not compromise their information privacy. Users believe that the application has complied with the existing laws and regulations to maintain user information privacy. Similarly, the third hypothesis, which stated that trusting beliefs will be negatively associated with risk beliefs, is also rejected. Other studies conducted by Kusyanti et al. [11] and Kuo et al. [15] stated that the more users declared that they have trust in social media, the less likely users believe a risk on the social media. Lastly, the fifth hypothesis, which stated that risk beliefs would be negatively associated with behavioral intention to provide personal information on Instagram, is also rejected. Another study proved that perceived vulnerability increases privacy concerns [17]. Individuals who experience positive things resulting from sharing information on Instagram, such as getting a job offer, will argue that sharing information on Instagram does not raise information privacy issues. Perceptions of vulnerability can vary depending on a person's experience. Meanwhile, another research states that decision making is influenced by experiences which influence risk preferences [27].

This research recommends that educational institutions increase students' awareness and concern for information privacy by conducting an information security awareness campaign. The campaign could be conducted step by step, starting from improving students' knowledge of the importance of information privacy awareness, the possible misuse of personal information, and how to protect their personal information. These activities could be done by spreading posters, infographics via social media, seminars, a welcome party for new students, installing banners, and Videotron.

VI. CONCLUSIONS

This study's primary purpose is to examine the information privacy concerns among Instagram users in Indonesia, more specifically amongst college students, who are the largest user group of Instagram in Indonesia. Our finding confirms that although users are aware of the risk of information misuse by using Instagram, it does not affect their intention to use Instagram. Other factors influence Indonesian college students' trust, such as Instagram's reputation, the number of users who use Instagram, the ease of using Instagram, the skills and knowledge of Indonesian students about Instagram, and the privacy settings that Instagram has. Furthermore, Indonesian college students tend to ignore the risk awareness they have if they already have trust in Instagram. Thus, the intention of Indonesian college students to use and share personal information on Instagram is positively influenced by trust factors towards Instagram. In conclusion, Indonesian college students' awareness and concern for information privacy will significantly influence the increased awareness of risk awareness privacy. However, the students' intention to risk awareness does not directly affect Indonesian college students' behavior to share their personal information.

Respondents in this study have experienced in using Instagram for one to seven years. Only 13 respondents (3%) had less than one year of experience. This study's limitation is that the research's respondents are only taken from students of Institut Teknologi Sepuluh Nopember (ITS, in English: Tenth of November Institute of Technology). Further research is needed to investigate whether this result is applied for students in other universities in Indonesia.

ACKNOWLEDGMENTS

We would like to thank the Research Center of Institut Teknologi Sepuluh Nopember (ITS), Surabaya-Indonesia, for supporting this research under the "Young Researcher Grant" for the year of 2019, contract number 1229/PKS/ITS/2019.

REFERENCES

[1] J. Clement, "Leading countries based on number of Instagram users as of October 2019 (in millions)," Statista, 20 November 2019. [Online]. Available: https://www.statista.com/statistics/578364/countries-with-most-instagram-users/. [Accessed 3 December 2019].

[2] NapoleonCat, "Instagram users in Indonesia," February 2019. [Online]. Available: https://napoleoncat.com/stats/instagram-users-in-indonesia/2019/02.

[3] Y. Li, "The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns," Decision Support Systems, vol. 57, pp. 343–354, 2014.

[4] J. Bryce and M. Klang, "Young people, disclosure of personal information and online privacy: Control, choice and consequences," Information Security Technical Report, vol. 14, no. 3, pp. 160-166, 2009.

[5] L. A. Bygrave, DATA PROTECTION LAW: Approaching Its Rationale, Logic and Limits, New York: Kluwer Law International, 2002.

[6] M. Klang, "Spyware – the ethics of covert software," Ethics and Information Technology, vol. 6, pp. 193–202, 2004.

[7] S. Livingstone, "Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression," New Media and Society, vol. 10, no. 3, pp. 393-411, 2008.

[8] N. K. Malhotra, S. S. Kim and J. Agarwal, "Internet users's information privacy concerns (IUIPC): The construct, the scale, and a causal model," Information Systems Research, vol. 15, no. 4, pp. 336, 2004.

[9] K. A. Stewart and A. H. Segars, "An Empirical Examination of the Concern for Information Privacy Instrument," Information Systems Research, vol. 13, no. 1, pp. 36-49, 2002.

[10] J. C. Sipior, B. T. Ward and R. Connolly, "Empirically assessing the continued applicability of the IUIPC construct," Journal of Enterprise Information Management, vol. 26, no. 6, pp. 661-678, 2013.

[11] A. Kusyanti, D. R. Puspitasari, H. P. A. Catherina and Y. A. L. Sari, "Information Privacy Concerns on Teens as Facebook Users in Indonesia," in 4th Information Systems International Conference, Bali, 2018.

[12] K. Finstad, "Response Interpolation and Scale Sensitivity: Evidence Against 5-Point Scales", Journal of Usability Studies, vol. 5, no. 3, pp. 104-110, May, 2010.

[13] I. Ghozali, Model Persamaan Struktural Konsep dan Aplikasi dengan Program AMOS 24, 7th edition, Semarang: Badan Penerbit Universitas Diponegoro, 2017.

[14] M. Waluyo, Mudah Cepat Tepat Penggunaan Tools AMOS dalam Aplikasi SEM, Surabaya: UPN Jatim, 2016.

[15] H. J. Smith, T. Dinev and H. Xu, "Information privacy research: an interdisciplinary review," MIS Quarterly, vol. 35, no. 4, pp. 989-1015, December 2011.

[16] K.-M. Kuo and P. C. Talley, "An Empirical Investigation of The Privacy Concerns of Social Network Site Users in Taiwan," International Journal of Scientific Knowledge, vol. 5, no. 2, pp. 1-19, June 2014.

[17] S. Öhman, "Previous Experiences and Risk Perception: The Role of Transference," Journal of Education, Society and Behavioural Science, pp. 1-10, 2017.

[18] T. Dinev and P. Hart, "Internet privacy concerns and their antecedents - measurement validity and a regression model," Behaviour and Information Technology, pp. 413-422, 2004.

[19] P. Kusev, "Understanding Risky Behavior: The Influence of Cognitive, Emotional and Hormonal Factors on Decision-Making under Risk," Frontiers in Psychology, pp. 1-28, 2017.

[20] J. L. Monforti and J. Marichal, "The Role of Digital Skills in the Formation of Generalized Trust Among Latinos and African Americans in the United States," Social Science Computer Review, pp. 3-17, 2014.

[21] P. Håkansson and H. Witmer, "Social Media and Trust — A Systematic Literature Review," Journal of Business and Economics, pp. 517-524, 2015.

[22] L. Rong, J. J. Kim and J. S. Park, "The Effects of Internet Shoppers' Trust on Their Purchasing Intention in China," Journal of Information Systems and Technology Management, pp. 269-286, 2007.

[23] C. E. Beaudoin, "Explaining the Relationship between Internet Use and Interpersonal Trust: Taking into Account Motivation and Information Overload," Journal of Computer-Mediated Communication, pp. 550-568, 2008.

[24] B. Ganguly, S. Dash and D. Cyr, "Website characteristics, Trust and purchase intention in online stores: - An Empirical study in the Indian context," Journal of Information Science and Technology, pp. 23-44, 2009.

[25] N. Afiah, "Pengaruh Keamanan, Reputasi dan Pengalaman Terhadap Trust Pengguna Internet Untuk Bertransaksi Secara Online," Jurnal Ekonomi dan Pendidikan, pp. 58-65, 2018.

[26] F. Herzallah and M. Mukhtar, "The Impact of Percieved Usefulness, Ease of Use and Trust on Managers' Acceptance of e-Commerce Services in Small and Medium-Sized Enterprises (SMEs) in Palestine," International Journal on Advanced Science, Engineering and Information Technology, pp. 922-929, 2016.

[27] P. Kusev dkk., "Understanding Risky Behaviour: The Influence of Cognitive, Emotional and Hormonal Factors on Decision-Making Under Risk," Front. Psychol., vol. 8, no. 102, pp. 1–28, 2017.