ISSN 2278-3091
Volume 8, No.1.5, 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse4981.52019.pdf
https://doi.org/10.30534/ijatcse/2019/4981.52019

Is Information Privacy Awareness Important for Indonesian Social Media Instagram Users?

Candiwan[1], Faiz Savindraputra[2]
[1]Telkom University, Indonesia, candiwan@telkomuniversity.ac.id
[2] Telkom University, Indonesia, faiz.savindra@gmail.com

ABSTRACT

In the current information technology era, social media users increase every year. Recorded in 2017, among 143.26 million internet users, 87.13% or about 124.82 million used social media as part of lifestyle. There are some crimes such as robberies and murder happen caused by posting pictures or video regarding the privacy of Instagram users. In this research, there are some actions that users can do to avoid the crimes. This research aims to measure the privacy awareness of Instagram users in Indonesia by doing measurement using three dimensions of awareness such as Attitude, Knowledge, Behavior with four focus areas of privacy, namely Perceived Surveillance, Perceived Intrusion, Secondary Use of Information, Disclosing Personal Information. This research used the Analytical Hierarchy Process (AHP) method to measure the privacy awareness of Instagram users in Indonesia. Privacy awareness level in all dimensions is good. However, the attitude dimension with focus areas on perceived surveillance and perceived intrusion is still in the criterion of average awareness. It means that those focus areas potentially need treatment to improve such as being more careful while posting some content on Instagram because unauthorized people can get access more easily to the user's personal information and the users' activities.

Key words: Attitude, behavior, knowledge, privacy awareness.

1. INTRODUCTION

In the current information technology era, social media users increase every year. Recorded in 2017, among 143.26 million internet users, 87.13% or about 124.82 million used social media as part of lifestyle [1]. Indonesia is the largest Instagram Story producing country in the world, with twice as much content as the global average [2]. Indonesia is the country with the largest Instagram users in the Asia Pacific region. Instagram grabs 700 million monthly active users globally, in which 45 million of them are from Indonesia [3]. The large number of social media users and the convenience offered can cause risk to the users [4]. The growth of Instagram users in Indonesia entails users to be more careful in using Instagram.

Lack of privacy awareness bring some case for social media users. For example, a man is named Tony Harris, 50 years old was killed by a group of robbers because he uploaded a photo on Instagram story containing his wife holding a stack of money [5]. As told by police commissioner Bayu Soeseno, a brief mode of robbers and thieves often monitor their prey from social media. Criminals use various methods or modes to get their targets. The perpetrators simply look at 15 photos on Facebook or Instagram to find out that the victim was currently enjoying a long vacation far away from home [6]. There are facts that show the misuse of personal data as part of individual privacy has the potential to be a serious problem. The average global cost of cybercrime increased more than 27 percent in 2017 [7]. The average cost of loss per user is around $ 141 because of the loss or theft of their personal data [8]. The application category with the biggest problem with cybersecurity is lifestyle applications, with a figure of 27% [9].

Privacy, for the most part, is another human right, so privacy concern is not spared from the government's surveillance. Lately, increasing information sharing tools make the right to privacy has serious attention [10]. As the Minister of Communication and Information regulation Republic Indonesia Number 20 in 2016 concerning personal data protection in electronic system in article 1 paragraph 1. It stated that personal data is certain personal data that is stored, maintained well and protected confidentially. Clarified in article 2 paragraph 2 point, respect for personal data is privacy. The heart of privacy issues is identity that might contain social security number, full name or residence address [11]. Data used to identify someone can be categorized as personal data [12].

Based on the explanation above, we researched by measuring privacy awareness to remind users of the negative impact they can get when posting some content on Instagram.

2. THEORETICAL BACKGROUND

Developing a measuring instrument based on techniques on the field of social psychology proposes that the tendency to learn response to certain objects beneficial or unfavorable has three components, which are Affect, Behavior, and Cognition [13]. These three components are used as the basis and the model and developed on three equal dimensions, namely what someone knows (Knowledge), how they feel about the topic (Attitude), and what they do (Behavior) [13].

Privacy is often associated with the ability of an individual to control the conditions under which personal information is obtained and used [14]. When sharing information, individuals must consider losses and the advantages of spreading information [15]. There are four approaches to define information privacy (a) privacy as human rights, (b) privacy as a commodity, (c) privacy as a state of limited access, and (d) privacy as the ability to control information about yourself [13]. Measurement of consciousness is measured by four sub-variables, namely (a) Perceived Surveillance (b) Perceived Intrusion (c) Secondary Use of Information (d) Disclosing Personal Information [16].

Perceived Surveillance which is the practice of collecting data both legal and illegal is the beginning of violations of privacy. Perceived Surveillance is a means to view, study, or record the behavior of each user. In the current digital era, some irresponsible parties use technology to track profiles of users [16].

Perceived Intrusion is an action that disturbs calmness or convenience and involves the presence or activity of others [16]. Perceived Intrusion is a flow of users' information that is not controlled by the users that can make them uncomfortable and harmful [16].

Secondary Use of Information is the use of personal information in which information is collected for other purposes without permission of the owner of the information [16]. The activity of using secondary information by other parties can potentially endanger individual ability in keeping their personal information [16].

The focus area of Disclosing Personal Information is something that describes several factors that are reasons why users disclose their personal information. [14]. Internet users have different behaviors in response to concerns about to which extent they are willing to share their personal information [14]. Many studies show that there is a gap between users' concerns about the risk of violating their privacy and their willingness to disclose their personal information to other parties. This gap is called "the privacy paradox" and explained by three variables : (1) various material or social benefits that can be obtained by users when disclosing their personal information (2) differences in the level of trust that users have when using internet (3) awareness of specific characteristics of internet technology and its risks [14].

3. METHOD

The type of this research is quantitative, in which data is collected by using a questionnaire which is spread through google form. This research uses a nominal scale type and dichotomous scaling method. Validity test is used to determine the feasibility of the items in the questionnaire in defining a variable [17]. Nominal scale is a scale that is used to classify an object or event into a particular group so that it can be observed similarities and differences over certain characteristics [18]. Simple category scale offers two choices one must choose [19]. The population in this research is not known exactly, therefore to determine the sample in this research Bernoulli formula is used with the calculation as below.

$$n = \frac{Z\frac{2}{C.\ 1}pq}{e^2} \quad (1)$$

n = Minimum sample amount
Z = Square of confidence interval
α / 2 = Acceptable level of trust (95% = 1.96)
e = Error rate that is still acceptable
p = Estimated proportion of success
q = Estimated proportion of failure / 1 – p

This research used a confidence level of 95% so that the value of Z = 1.96 is obtained. The error rate is set at 5%. By substituting these values in the equations that have been provided, they are obtained.

$$n = \frac{(1.96)^2(0.5)(0.5)}{0.05^2}$$

$$- \frac{(3.8416)(0.25)}{0.0025}$$

$$= \frac{0.9604}{0.0025}$$

$$- 384.16 - 384$$

From the results of the calculation above, Bernoulli's formula required at least 384 samples. Therefore, to facilitate the process of further counting, the number of respondents to be taken in this research is 400 people.

This research has 36 questions about privacy awareness to test attitude, knowledge, and behavior of Instagram users. Some questions are answered on a 3-point scale consisting of "yes", "do not know", and "no" (attitude and knowledge), while others only require answers "yes" or "no" (behavior). These are some examples of questions from each dimension that can be seen in Table 1.

Table 1: Sample Question

Dimension	Statement	Answer
Attitude	I am worried if I use Instagram, the personal information that I have can be collected (A1.2).	1. Yes 2. Don't Know 3. No
Knowledge	I know that by using Instagram, the personal information that I share (such as name, address, age, location, habits, content, messages, etc.) can be collected (B1.2).	1. Yes 2. Don't Know 3. No
Behavior	I read the provisions of the data to be collected by Instagram when creating an Instagram account (C1.2).	1. Yes 2. No

To perform the validity and reliability test of the questionnaire in this research, we used 30 samples of respondents. Validity test in this research used Product Moment correlation technique. By using the r table value with n = 30 and the significance level of 5%, the r-value of the table obtained is 0.361. The following are the results of the validity tests that have been conducted on the questionnaire.

Table 2: The Results of Privacy Awareness Validity Test

Statement Item	Item Code	Validity Test		Kategori
		R. Table	R. Count	
Attitude_P1	A1.1	0.361	0.681	Valid
Attitude_P2	A1.2	0.361	0.664	Valid
Attitude_P3	A1.3	0.361	0.465	Valid
Attitude_P4	A2.1	0.361	0.372	Valid
Attitude _P5	A2.2	0.361	0.786	Valid
Attitude _P6	A2.3	0.361	0.661	Valid
Attitude _P7	A3.1	0.361	0.876	Valid
Attitude _P8	A3.2	0.361	0.934	Valid
Attitude _P9	A3.3	0.361	0.823	Valid
Attitude _P10	A4.1	0.361	0.734	Valid
Attitude _P11	A4.2	0.361	0.704	Valid
Attitude _P12	A4.3	0.361	0.905	Valid
Knowledge_P1	B1.1	0.361	0.410	Valid
Knowledge_P2	B1.2	0.361	0.694	Valid
Knowledge_P3	B1.3	0.361	0.406	Valid
Knowledge_P4	B2.1	0.361	0.851	Valid
Knowledge_P5	B2.2	0.361	0.810	Valid
Knowledge_P6	B2.3	0.361	0.914	Valid
Knowledge_P7	B3.1	0.361	0.922	Valid
Knowledge_P8	B3.2	0.361	0.896	Valid
Knowledge_P9	B3.3	0.361	0.922	Valid
Knowledge_P10	B4.1	0.361	0.794	Valid
Knowledge _P11	B4.2	0.361	0.811	Valid
Knowledge_P12	B4.3	0.361	0.908	Valid
Behavior_P1	C1.1	0.361	0.545	Valid
Behavior_P2	C1.2	0.361	0.373	Valid
Behavior_P3	C1.3	0.361	0.884	Valid
Behavior_P4	C2.1	0.361	0.645	Valid
Behavior_P5	C2.2	0.361	0.694	Valid
Behavior_P6	C2.3	0.361	0.676	Valid
Behavior_P7	C3.1	0.361	0.884	Valid
Behavior_P8	C3.2	0.361	0.884	Valid
Behavior_P9	C3.3	0.361	0.519	Valid
Behavior_P10	C4.1	0.361	0.795	Valid
Behavior_P11	C4.2	0.361	0.583	Valid
Behavior_P12	C4.3	0.361	0.795	Valid

This reliability test uses the Cronbach Alpha technique with the help of IBM SPSS Statistics 23 application. If r count > r table then the question is declared reliable, if r count ≤ r table then the question is declared unreliable. With a confidence level of 95%, the results are obtained.

Table 3. Test Results for the Reliability of Privacy Awareness

Cronbach's Alpha	N of Items	Category
0,963	36	Reliable

The dimensional research framework and focus areas are adapted from Akraman [20] and the addition of a focus on the Disclosing Personal Information area is based on the Privacy Paradox theory [14]. Three components use to measure beneficial or unfavorable ways towards certain objects adapted from social psychology theory [13]. The component is used to develop three dimensions known as attitude (knowledge), knowledge (one's knowledge), and behavior (someone's behavior) [13]. Each dimension is divided into four focus areas. The Following figure is the research framework adopted from [20] shown in Figure 1.

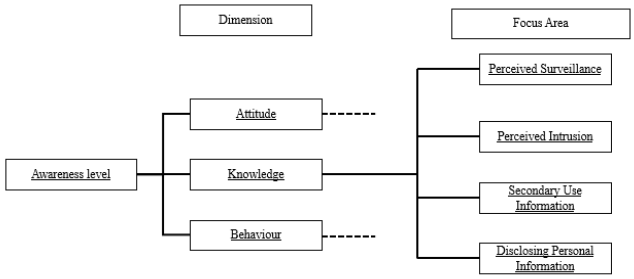

Figure 1: Research Framework

The framework of privacy awareness research in Figure 1 with adoption from [20] to measure the level of awareness was adapted from Xu [16] called perceived surveillance, perceived intrusion, and secondary use of information. Each focus area will be made from several adapted indicators [20]. The focus of the Disclosing Personal Information area is adapted from Ginosar [14]. Disclosing Personal Information is used to measure actions that provide material and social benefits that can be obtained by users when revealing personal information, different levels of trust that users have when doing specific activities on Instagram, and feelings for specific characteristics of internet technology [14].

The Focus areas, perceived surveillance, perceived intrusion, secondary use information, and disclosing personal information, were used as a measure of the privacy awareness of Instagram users. From the framework of the above research, several question indicators will be made from each focus area in this research.

Measuring the scale of privacy awareness is done by the Analytic Hierarchy Process (AHP) method. Because there is more than one focus area in the privacy sub-variable, the focus areas are measured by sub-variables contained in the Awareness variable, Attitude, Knowledge, Behavior. This AHP approach is used to weight each focus area and dimension according to the level of importance. The AHP approach uses paired comparisons to provide a subjective evaluation of factors based on expert judgment and professional opinion [13]. Comparisons are made using a preference scale, which gives numerical values to various preference levels [13].

Table 4: Dimension Weighting Value

Dimension	Weighting Value
Attitude	20%
Knowledge	30%
Behavior	50%

The dimensions of behavior need more attention and are followed by the dimensions of knowledge and attitude [13]. Weighting is carried out before calculation based on predetermined weights. Weighting is done on each dimension (attitude, knowledge, and behavior) and focus areas (perceived surveillance, perceived intrusion, secondary use of information, and disclosing personal information). The weighting value of the focus areas is done by assuming that each focus area has the same level of importance. The following are the focus areas weighting stages.

Table 5: Weighting of Importance in Focus Areas

	Perceived Surveillance	Perceived Intrusion	Secondary Use of Information	Disclosing Personal Information
Perceived Surveillance	1	1	1	1
Perceived Intrusion	1	1	1	1
Secondary Use of Information	1	1	1	1
Disclosing Personal Information	1	1	1	1
Total	4	4	4	4

Table 6: Normalization of Weighting Of Importance in Focus Areas

	Perceived Surveillance	Perceived Intrusion	Secondary Use of Information	Disclosing Personal Information	Average
Perceived Surveillance	25 %	25%	25%	25%	25%
Perceived Intrusion	25 %	25%	25%	25%	25%
Secondary Use of Information	25 %	25%	25%	25%	25%
Disclosing Personal Information	25 %	25%	25%	25%	25%
Total	1	1	1	1	100%

Table 6 shows the results of weighting normalization of interest shown in Table 5.

Table 7: Focus Area Weighting Value

Focus	Weighting Value
Perceived Surveillance	25%
Perceived Intrusion	25%
Secondary Use of Information	25%
Disclosing Personal Information	25%

Focus area weighting values is obtained by assuming that each focus area has the same level of importance with the results shown in Table 7. The weight of importance obtained by the AHP approach uses paired comparisons to provide subjective evaluations of factors based on professional considerations and opinions [13]. Bases on table 4 and table 7, we calculate the value of privacy awareness in each

dimension, focus area, and total. Comparisons are carried out using a preference scale, which gives numerical values to various preference levels.

Table 8: Awareness Criteria

Criteria	Value	Action
Good	77,78% - 100%	Action is not needed
Average/ Satisfactory	55,56% - 77,77%	Potential actions are needed
Poor	33,33% - 55,55%	Action is needed

The score of each focus area and later dimensions is grouped as the consciousness criteria in accordance with Table 8. The interval value of criteria is based on the value of the continuum line in which the maximum value is 100% and the minimum score is 33.33% [21]. Every criterion to identify focus areas requires action to improve or not [21]. After calculating the predetermined weights, the results are obtained in the form of privacy awareness criteria in each focus area and dimension in this research. Every result of privacy awareness criterion has actions that need to be carried out at a later stage when privacy awareness is on certain criteria. Weighting on privacy is done using the analytical hierarchy process (AHP) method. The result scores for each dimension and focus areas are then grouped as awareness criteria in Table 12.

4. RESULTS AND DISCUSSION

This research took samples with 400 respondents in which the questionnaire was distributed by the researcher in March 2019 in Indonesia. The following table is characteristic of the respondents who use Instagram.

Table 9: Respondent gender

Sex	Number of Respondents	Percentage
Male	148	37%
Female	252	63%

Table 10: Respondent age

Age	Number of Respondents	Percentage
16 - 18 year	43	10.75%
19 - 23 year	291	72.75%
24 - 30 year	10	2.5%
31 - 40 year	15	3.75%
41 - 50 year	30	7.5%
>50 year	11	2.75%

Based on table 10 above, out of the 400 samples, the age of respondents from the ages of 16-18 years was 43 respondents (10.75%). Respondents aged 19-23 years were 291 respondents (72.75%). Respondents aged 24-30 were 10 respondents (2.5%). Respondents aged 31-40 were 15 respondents (3.75%). And respondents aged over 50 years were 11 respondents (2.75%). Based on this data, it can be concluded that the age range of 19-23 years is the age range of Instagram users who dominated the research. Compared to other research, most respondents also came from young people [20].

Table 11: Respondent Profession

Profession	Number of Respondents	Percentage
Freelance	4	1%
Housewife	3	0.75%
College student	298	74.5%
BUMN employee	2	0.5%
Civil Servant	3	0.75%
Private Officer	73	18.25%
Entrepreneur	17	4.25%

Table 12: Privacy Awareness Level

Dimension	ATTITUDE	KNOWLEDGE	BEHAVIOR	Total Awareness / Focus areas
Focus areas	**(20%)**	**(30%)**	**(50%)**	
Perceived Surveillance (25%)	73.41%	78.67%	79.33%	**77.14%**
Perceived Intrusion (25%)	75.83%	83.42%	89.33%	**82.86%**
Secondary Use of Information (25%)	85.17%	86%	90.58%	**87.25%**
Disclosing Personal Information (25%)	78.67%	83.08%	88.25%	**83.33%**
Total Awareness / Dimension	**78.27%**	**82.79%**	**86.87%**	**82.65%**

The level of privacy awareness in table 12 was used to present the results and findings obtained from the questionnaire filled by 400 respondents. Awareness criteria can provide

groupings according to criteria of focus areas that do not require action for improvement, potentially need action for improvement, and require action for improvement. Based on the level of privacy awareness in Table 12, the results according to the dimension are as follows.

The percentage of privacy awareness is 82.65%. It shows that the level of privacy awareness is in the good criteria. In this level, the respondents do not need treatment to improve their privacy awareness. Based on other researches, the overall level of privacy is in the average criteria with the respondents who use an android smartphone [20]. Overall privacy awareness in the Australian region whose respondents are official employees is 65% [13].

The highest percentage of awareness is the behavior dimension which is 86.87%. In this level, the respondents do not need treatment to improve their behavior. It happens because users notice which important information they will share on Instagram to avoid disruption of privacy. They also consider which information they provide to get benefit when sharing their personal information, even though they don't read the terms of the data that will be collected by Instagram when creating an account.

The percentage of knowledge dimension is 82.79% which is a good level of awareness. The respondents do not need treatment to improve their knowledge. It happens because users know that by using Instagram, their personal information can be used for other purposes without getting their permission. And then, they cannot be certain what benefit they will receive when they disclose the personal information they have.

The smallest percentage of awareness is the attitude dimension which is 78.27%. Respondents do not need treatment to improve their attitude. It happen because user notice that personal information can be used for other purposes. Although there are some respondent do not mind if there are people they do not want to know their personal information. Besides, they also feel the consequences of using the Instagram application.

Level of privacy awareness in all dimensions including the criteria of good awareness, the dimensions of attitude with area focus perceived surveillance and perceived intrusion is still included in the criteria of average awareness and potentially requires action for improvement. Compared to other researches, although the lack of user knowledge of the use of personal information applications can be known, the user has chosen which information to share [20]. Based on the results in this research, there are similarities in results, in which the dimension of behavior is the highest level of awareness.

Based on the level of privacy awareness in Table 12, the results according to the focus areas are as follows.

The percentage of perceived surveillance is 77.14% which is an average criteria. The percentage of attitude dimension is 73.41% which is an average criteria so that treatment is needed. It happens because there are two indicators in the average criteria. First, some users do not believe that the location feature on the mobile phone is activated so that all activities they do can be identified on Instagram. Second, some users are not worried if they use Instagram and post photos or videos so, their activities can be identified. Based on another research, the level of perceived surveillance in the attitude dimension is in the average criteria [20].

The percentage of perceived intrusion is 82.86% which is the good criteria. However, the percentage of attitude dimension is 75.83% which is the average criteria so that treatment is needed. It happens because there are two indicators that are in the average criteria. First, some users feel comfortable because using Instagram can cause unauthorized parties to know about their personal information. Second, some users do not believe that by using Instagram, the personal information that they have is more easily available to unauthorized parties. Compared to other research, perceived intrusion on all dimensions is in the average criteria [20].

The percentage of secondary use of information is 87.25% which is good criteria. In this level, the respondents do not need treatment. It happens because users notice that personal information can be used for other purposes. Based on other researches, secondary use of information in the dimensions of attitude and behavior already have good awareness criteria, but the knowledge dimension has average awareness criteria [20] [22] [23]. Perceived surveillance, perceived intrusion, and secondary use of information can describe each dimension [16].

The percentage of disclosing personal information is 83.33% in good criteria. In this level, the respondents do not need treatment. It happens because users always consider which information they will provide to get benefit when sharing their personal information (such as name, address, age, location, habits, content, messages, etc.) on Instagram. There is no single focus area or dimension of the level of privacy awareness that is included in the criteria of poor awareness (awareness level below 55.56%).

5. CONCLUSION

Based on the results of our research, overall, the level of privacy awareness of Instagram users in Indonesia is included in the good criteria (82.65%). Attitude dimension level of privacy awareness on Instagram users an in the good criteria (78.27%). However, focus perceived surveillance (73.41%) and perceived intrusion (75.83%) in this dimension have the potential to be given a corrective action so that the focus area can be categorized in the criteria of good awareness. It happens because some users are too careless when using Instagram in which the personal information that they have is more easily available to unwanted parties. Knowledge and behavioral dimension levels of privacy awareness of Instagram users are included in the good criteria and there is no focus area in these dimensions that below the good criteria. Based on this research, there are some actions that users can do to avoid crime such as (1) Being more careful when posting something on Instagram on which their activities can be identified. (2) Increasing the sense of caution because the use of instagram causes unauthorized parties to know the user's personal information.

REFERENCES

1. APJII. (2017). Penetrasi & Perilaku Pengguna Internet Indonesia. Retrieved from www.teknopreneur.com
2. Tempo.co. (2017). 45 Juta Pengguna Instagram, Indonesia Pasar Terbesar di Asia - Bisnis Tempo.co. Retrieved January 28, 2019, from https://bisnis.tempo.co/read/894605/45-juta-pengguna-instagram-indonesia-pasar-terbesar-di-asia
3. Kartini Bohang, F. (2017). Indonesia, Pengguna Instagram Terbesar se-Asia Pasifik - Kompas.com. Retrieved January 28, 2019, from https://tekno.kompas.com/read/2017/07/27/11480087/indonesia-pengguna-instagram-terbesar-se-asia-pasifik
4. Mishna, F., Saini, M., & Solomon, S. **Ongoing And Online: Children and Youth's Perceptions of Cyberbullying.** *Children and Youth Services Review*, Vol. 31, Issue 12, pp. 1222–1228, December 2009. https://doi.org/10.1016/j.childyouth.2009.05.004
5. Pradita Abbas, F. (2017). Gara-gara Pamer Foto Uang Ratusan Juta di Facebook, Pria Ini Langsung Dibunuh - Tribun Jabar. Retrieved January 28, 2019, from http://jabar.tribunnews.com/2017/09/03/gara-gara-pamer-foto-uang-ratusan-juta-di-facebook-pria-ini-langsung-dibunuh
6. Tumanggor, A. (2017). Perampok Lakukan Pemantauan dari Medsos, Berikut Tips Antisipasinya yang Dibagikan Polisi Bayu - Tribun Medan. Retrieved January 28, 2019, from http://medan.tribunnews.com/2017/08/29/perampok-lakukan-pemantauan-dari-medsos-berikut-tips-antisipasinya-yang-dibagikan-polisi-bayu
7. Sobers, R. (n.d.). 60 Must-Know Cybersecurity Statistics for 2019. Retrieved May 22, 2019, from https://www.varonis.com/blog/cybersecurity-statistics/
8. 2017 Cost of Data Breach Study Global Overview. (2017). Retrieved from https://www.ibm.com/downloads/cas/ZYKLN2E3
9. ISTR Internet Security Threat Report Volume 23. (n.d.). Retrieved from http://images.mktgassets.symantec.com/Web/Symantec/%7B3a70beb8-c55d-4516-98ed-1d0818a42661%7D_ISTR23_Main-FINAL-APR10.pdf?aid=elq_
10. Fayad, M. E., Kuppa, G., & Hamu, D. (2019). **Unified and Stable Privacy Model.** *International Journal of Advanced Trends in Computer Science and Engineering*, Vol. 8, no. 1.4, pp. 515 -521. https://doi.org/10.30534/ijatcse/2019/8081.42019
11. Ajami, R., Al Qirim, N., & Ramadan, N. **Privacy Issues in Mobile Social Networks**. *Procedia Computer Science*, Vol. 10, pp. 672–679, December 2012. https://doi.org/10.1016/j.procs.2012.06.086
12. Hendriyani, Y., Jalinus, N., Delianti, V. I., & Mursyida, L. **Analisis Kebutuhan Pengembangan Media Pembelajaran Berbasis Video Tutorial.** *Jurnal Teknologi Informasi dan Pendidikan*, Vol. 11, no.2, pp. 2–5, November 2018.
13. Kruger, H. A., & Kearney, W. D. **A Prototype For Assessing Information Security Awareness.** *Computers & Security*, Vol. 25, Issue 4, pp. 289–296, June 2006. https://doi.org/10.1016/j.cose.2006.02.008
14. Ginosar, A., & Ariel, Y. **An Analytical Framework For Online Privacy Research: What is Missing?** *Information and Management*, Vol. 54, Issue 7, pp. 948–957, November 2017. https://doi.org/10.1016/j.im.2017.02.004
15. Wottrich, V. M., van Reijmersdal, E. A., & Smit, E. G. **The Privacy Trade-Off For Mobile App Downloads: The Roles of App Value, Intrusiveness, and Privacy Concerns.** *Decision Support Systems*, Vol. 106, pp. 44–52, February 2018. https://doi.org/10.1016/j.dss.2017.12.003
16. Xu, H., Gupta, S., Rosson, M. B., & Carroll, J. M. **Measuring Mobile Users' Concerns for Information Privacy,** in *Proc. Thirty Third International Conference on Information Systems*, Orlando, 2012, pp. 1–16.
17. Sujarweni, V. W. **Metodologi Penelitian Bisnis & Ekonomi.** Yogyakarta: Pustaka Baru Pres, 2015.
18. Indrawati. **Metode Penelitian Manajemen dan Bisnis: Konvergensi Teknologi Komunikasi dan Informasi.** Bandung: Refika Aditama, 2015.
19. Cooper, D. R., & Schindler, P. S. **Metode Riset Bisnis.** R. Dewi, Ed. 9th Ed. Jakarta: Media Global Edukasi, 2006.
20. R. Akraman, C. Candiwan, and Y. Priyadi, **Pengukuran Kesadaran Keamanan Informasi dan Privasi Pada Pengguna Smartphone Android di Indonesia**, *JSINBIS (Jurnal Sistem Informasi Bisnis)*, Vol. 8, no. 2, pp. 115-122, October 2018. https://doi.org/10.21456/vol8iss2pp115-122
21. Sari, P. K., & Candiwan, C. **Measuring Information Security Awareness of Indonesian Smartphone Users.** *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, Vol. 12, no. 2, pp. 493, June 2014. http://dx.doi.org/10.12928/telkomnika.v12i2.64
22. P. Soundaryamala, D. G. Sankar, S. Ramakrishna, and S. T. P. Radika, "Initializing key for High Level Transformation for FIR filters," Int. J. Adv. Trends Comput. Sci. Eng., vol. 8, no. 1, pp. 78–81, 2019.
23. O. Al-omari and N. Omari, "International Journal of Advanced Trends in Computer Science and Engineering Enhanced Document Classification Using Noun Verb (NV) Terms Extraction Approach," vol. 8, no. 1, pp. 85–92, 2019.