Journal of Theoretical and Applied Information Technology
30th April 2019. Vol.97. No 8

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SMARTPHONE USER AWARENESS OF PERSONAL INFORMATION SECURITY AND PRIVACY

[1]JAROT S. SUROSO, [2]ANGGA RHYANDA PUTRA, [3]JEANIFER GUNAWAN, [4]DIONISIUS W. DANUANINDITO

[1-4]Master of Information System Management, Bina Nusantara University, Indonesia

E-mail: [1]jsembodo@binus.edu, [2]angga.putra008@binus.ac.id, [3]jeanifer.gunawan@binus.ac.id, [4]dionisius.danuanindito@binus.ac.id

ABSTRACT

The security of information from users of internet services in recent years has become a hot issue that continues to be reviewed, where researchers find that the privacy of personal information is no longer controlled by individual data or information owners but has changed hands to organizations which hold the data or information. In Indonesia alone, the issue of cyber security is certainly closely related to technological growth. In 2018 as many as 83.19% of Indonesia's population are active internet users and as many as 26.26% of Indonesia's population are smartphone users. When viewed positively, the use of technological developments can facilitate data collection so that existing data or information can be reused for interests that can benefit both organizations and individuals. This study aims to find out what factors influence smartphone users to open their personal information and provide access to mobile applications. These factors have been examined previously by Benson et al [1], which consists of 4 factors, namely Control Over Personal Information, Use of Information, and Privacy Notice that affect Information Disclosure, and using questionnaire techniques with 101 respondents. From the results obtained, it was found that the Personal Control Over, Use of Information, and Privacy Notice are the influential factors for individuals to open their information or not. In addition, when users know the function of information that is opened and get privacy notifications in advance, smartphone users will tend to open their personal information and give permissions to either mobile platforms or mobile applications to access personal information.

Keywords: *Smartphone, Control, Use of Information, Privacy Notice, Information Disclosure*

1. INTRODUCTION

In December 2018, CNN broadcast a video in which the CEO of Google, Sundar Pichai, was investigated by US congress participants related to data collection that Google had done so far.

In the video, several panelists gave several questions related to user data collection techniques carried out by Google through the application that was issued, such as from Android devices, email facilities, search engines where all of these sources were known to be able to record all user account activities.

The security of information from users of internet services in recent years has become a hot issue that continues to be reviewed, where researchers find that privacy of personal information is no longer controlled by individual data or information owners, but has changed hands to organizations that hold data or that information [2]

The issue of cyber security is certainly closely related to technological growth in Indonesia. In 2018 83.19% of Indonesia's population were active internet users and 26.26% of Indonesia's population were smartphone users [3]–[5]

If viewed positively, utilizing technological developments can facilitate data collection so that existing data or information can be reused for purposes that can benefit both organizations and individuals, but of course all of these can not only provide positive input and benefits but also come with consequence [6]

In fact, every individual does not intend to disclose data, but because of the many limitations that an individual has so that they do not know the right way to keep personal data or information private [2].

For the case in Indonesia, it was said that the awareness of smartphone users related to cyber security was still low [7], according to research conducted in Indonesia, this was due to the fact that

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the Indonesian people were still negligent in website maintenance and lack of safeguards on internet access used by organizations so that the threat continued to attack and most of these threats also evolved over time.

In 2016, staff of the Ministry of Communication and Information invited at a conference and he was talk about the importance of developing a culture that is aware of cyber security. He said that cyber security problems could not only be overcome by regulation and technology, but also with the development of a cyber security awareness culture.

Almost all countries face difficulties in investigating cyber security cases because they are anonymous, transnational, and organized. Cyber security is important because from the cyber side there are many things that can be attacked in an organization or even country such as attacks on vital infrastructure, severe damage, reputation, public security, etc. [8].

This study will discuss the awareness of the Indonesian people regarding data security and technology privacy in Indonesia through the measurement of several variables. The expectation of this study is can provide an overview of the attitudes and awareness of the Indonesian people regarding data privacy in the period January to February 2019.

2. LITERATURE STUDY

2.1 Information Security

Information security is a method commonly used by companies to maintain their privacy of important information. There are three main objectives in information security, namely confidentiality, availability, and integrity. In addition, there are four definitions of information privacy, namely privacy as human rights, privacy as a commodity, privacy as a state of limited access, and privacy as the ability to control information about oneself [9].

Regarding information security, it is known as 4R information security, namely: Right Information, Right People, Right Time and Right Form [10]. 4R settings are the most efficient way to maintain and control the value of information. Right Information refers to the accuracy and completeness of information that guarantees information integrity. Right People means that information is available only to entitled individuals who guarantee confidentiality. Right Time refers to the accessibility of information and its use at the request of the right entity, this guarantees availability. While Right Form refers to providing information in the right format. To maintain information security, 4R must be used appropriately. This means that confidentiality, integrity and availability must be reviewed when handling information [10].

There are some of the information security concepts which described by Chan, H., & Mubarak, S. (2011) [11], include:

a) Phishing

It is an attempt to obtain confidential information or carry out identity theft using e-mail or fake websites that mimic the site address or actual e-mail address. Phishing is a common threat to aspects of confidentiality of information security and therefore it is important for employees to be aware of the concepts and dangers

b) Spam

It is a commercial electronic letter or message that is not desired by the recipient. Spam is not only disturbing the recipient but has the potential to cause disaster or disrupt the system. For example, malicious code such as viruses or trojans often use Spam as a vehicle for distribution. Besides that, in Spam messages, sometimes it contains links that point to phishing sites. Therefore, it is important for employees or individuals to be aware of the concepts of Spam and related hazards.

c) Social Engineering

It is the use of non-technical means to carry out identity theft or to obtain confidential information. Attackers in this case can use a combination of psychological manipulation and imitation in order to encourage victims to be unwilling to provide confidential information. Because of the very human aspects of Social Engineering, it is not possible to prevent attacks using technical controls.

d) Strong Password

It is the key to authenticating users and to prevent unauthorized access to the system. Apart from Social Engineering and phishing practices, passwords can be obtained illegally by using two attacks, known as password cracking. The stronger the password, the longer it will take to solve it. A strong password will reduce the chance of a password attack carried out by the attacker. Existing technical controls are capable of making strong passwords, but not all information systems have that control, therefore

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

employees need awareness to believe that their passwords are strong enough.

e) Data or Information Integrity

Regarding the integrity aspects of information security has the following characteristics:

- Accuracy and truth, that is, information must be strong and correct in the sense that data must be appropriate and in accordance with reality, for example birth date data entered into the system may not have the possibility of error space.
- Trust, ensuring accuracy and truth will ensure that information stored in the system is a representation of reality so that one can trust that information.
- Applicability and timeliness, using birth dates for example, exact dates of birth are variables that change over time

f) Social Networking

Opinions that social media or networking sites like Facebook and Twitter as sources of leaked confidential information have become increasingly relevant in recent years. Social media can be a source of data leakage when employees disclose personal information and information relating to workplaces on social media sites.

2.2 Risk in Mobile Application

The use of smartphones to help with daily activities, such as accessing information in e-mails, social networks, health services, company applications to banking or other financial services [12][13], unconsciously opens a large gap for the security and privacy of user data [13].

A large number of security and privacy threats such as malware that can steal confidential user information can be very detrimental [14]. Therefore, data security and privacy present a serious problem for companies and smartphone users. According to Jain et al., [15] the following are the risk in mobile applications that are commonly found: insecure data storage, weak server-side controls, Insufficient transport-layer protection, client-side injection, poor authorization and authentication, improper session handling, security decisions via untrusted input.

2.3 Security Awareness

According to Akraman, R., Candiwan, C., dan Priyadi, Y. (2018), security awareness are controls and rules which designed to reduce incidents of violations of information security resulting from negligence or planned actions [9].

Security awareness can be interpreted as a situation where a person has good knowledge or ability in carrying out security practices when using internet networking sites and understands the importance of protecting personal data and/ or group data on behalf of an organization when deciding to use an internet network site [14].

By considering that many risk will be faced by today's smartphone users, they should increase security awareness of the privacy of their personal data [15].

3. RESEARCH METHODOLOGY

3.1 Hypothesis Development

Personal information, the use of information and disclosure of information has attracted the attention of various researchers. Research conducted by [16], mentions that privacy issues have been empirically validated and are used to measure privacy perceptions. Further research conducted by [2], after data has been obtained, the data will be shared with second parties such as credit companies, the government and a number of data integrators.

When violated, data is also shared with third parties. From the extent of sharing this unknown data, the age of the data seems to be unlimited and there is no attempt to limit the age of the data in most of the current situations. When new technologies come, like smart phones, the problems above will be exacerbated. These problems require new ways to look at privacy in the context of various types of transactions to better manage new data collected, partnerships sharing data and personal information.

a) Perceived Ability to Control Submitted Information

Privacy is not so much the absence of our personal data at the disposal of others as the control that we can exert over our most personal information, those facts that allow us to interweave relationships of respect, faith, love, or friendship [17].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

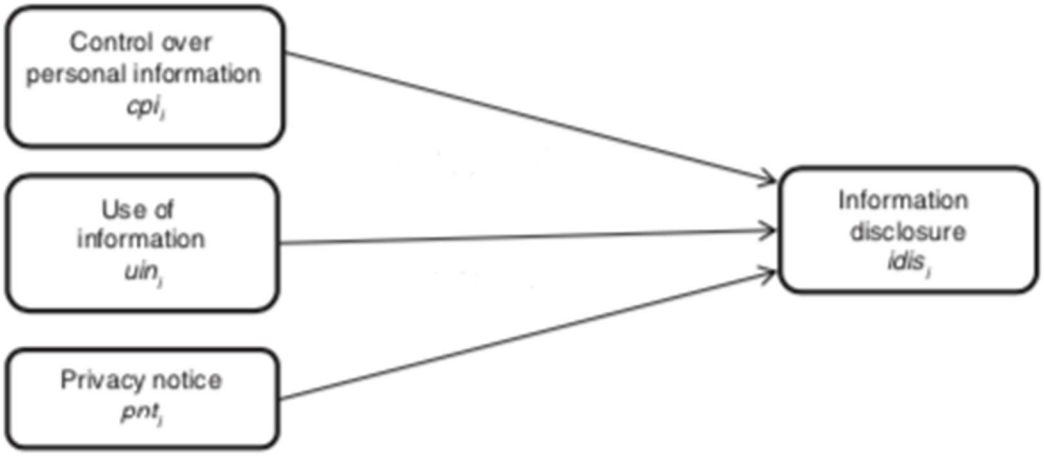

Figure 1. Information Disclosure Model [1]

A privacy right is an access control right over oneself. Privacy right also include a use or control feature that allows an exclusive use and control over personal information and specific bodies or locations [17].

The ability to adjust the sensors, interactional patterns and context representation are crucial in order to experimenting with privacy management. The system services status display keeps users aware of whether they are revealing personal information without having to navigate to other applications [18]. In the previous article written by [19], even though the smartphone approach puts the control in the user's hands, this does not protect the user from malicious applications.

For example, if the user downloads an ad-based application, then the application will send and receive text messages and the user must provide access to the application in form of Personal Information (to read contact data), All Messages (to read received messages), Network Communication (to download ads from the internet), and Services that Cost Money (sending messages can incur charges).

A legitimate application will only use these services for the intended purpose, but malicious software could use these services to communicate personal information to a website. According to the discussion of the literature that has been conducted, the following is the hypothesis proposed in this study:

H1: Personal information disclosures on smartphone can be reduced by user's high control over personal information.

b) Use of Information

The use of mobile applications this days, which is increasingly smart in serving smartphone users, actually has a very risk [15]. With reasons to facilitate daily activities of smartphone users, there are not a few mobile applications currently give smart services such as location readers, credit card details storage, electronic payment, and other financial services that make it possible to connect with user's bank account [13].

Although this action has a high level of risk, but in fact, many smartphone users use this service in their daily lives. Therefore, it can be hypothesized as follows:

H2: When the user of smartphone has more information about the use of their personal information, they will disclose their personal information

c) Privacy Notices

Notification to the user about the personal information that will be collected through information is effectively increase the individual's desire to use the mobile application [20]. Notices also plays an important part to deal with users' concerns about the possible risks of using mobile applications and according to some literature that discusses privacy notices, it is known that this

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

variable can increase the desire and trust of users to submit their personal data [21].

Actually, when the users have been given a notification about the terms and conditions, but the desire to read the terms and conditions is low due to the length of the letter that must be read by the user. Therefore it can be hypothesized as follows:

H3: The notification of privacy in smartphone usage increases the possibility of disclosing information/user data.

Basically, this research were conducted by referring to the research model that had been carried out previously by V. Benson et al [1].

In his research, V. Benson et al. using a research models as shown in Figure 1. What distinguishes this research from previous research is that this research will be conducted in Indonesia, especially JABODETABEK, where the awareness of mobile phone users to cyber security is still very low [7].

Please refer to Table 1 for variables and indicator used in this study.

3.2 Population and Sample

In aim to get empirical evidence, this study used questionnaire method for collects the data. The questionnaire that we made are designed for general respondents. The population used in this study are everyone who actively using smartphone, are domiciled in JABODETABEK (Jakarta, Bogor, Depok, Tangerang, and Bekasi) and those who were 17-50 years old. The reason why the population is limited by those aged 17-50 years because at this age level, they are considered to be responsible for themselves.

However, due to time and cost limitations, this study will only take a sample of 101 respondents and will be chose with random sampling technique.

3.3 Data Collection and Measures

The questionnaire will be distributed through online media, such as e-mail, social media and forums. All variables in this study were measured using a five-point Likert which the ranging from strongly disagree (1) to strongly agree (5).

After all questionnaires were collected, the data will be calculated using PLS-SEM technique. PLS-SEM technique was chosen in this study because this technique has been recognized that can facilitate the limitations of research where the sample size is small [22], [23].

In managing data, to ensure that the collected data can be processed and trusted, it is necessary to test validity and reliability in advance for all variables and indicators used in this study. Therefore, in testing validity and reliability in this study, we will use loading factors reference > 0.5 to measure variables validity and Composite Reliability > 0.7 to measure variables reliability [22].

After testing the validity and reliability, hypothesis testing will be carried out by looking at the numbers t-statistics and p-values as a reference whether the hypothesis is accepted or not.

The threshold of of t-statistics and p-values in this study are based on the criteria used by Kock [24]. Kock had explained that the hypothesis can be accepted if the t-statistic is above 1.96 and the p-value does not exceed 0.05.

Table 1. Variable and Indicator

Variables	Indicator
Control Over Personal Information [1]	1. Perceived ability to control over who can get access the personal information.
	2. Perceived ability to control over how personal information is used.
	3. Perceived ability to control personal information which was provided to mobile application or mobile platform (Google/ iOS).
Use of Information [1]	1. Authorization for giving personal information.
	2. The ability to forbid any third party from selling personal information.
	3. The ability to forbid any third parties from sharing personal information

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Privacy Notices [1]	1. Security features.
	2. The content of privacy policy that've been provided by third party
	3. The security seals of mobile platform

4. RESULTS AND ANALYSIS

4.1 Respondent's Demographic

From the survey conducted, 101 respondents successfully completed the questionnaire. The respondents' demographics have been presented in the form of a table which can be seen in Table 2.

The majority of respondents in this study were men with the percentage 57.43% and the rest were women. The majority of respondents were in the age group 26-30 years old or around 49.50%. And 83.17% of all respondents had occupation as employees and 83.17% of all respondents had undergraduate education. In addition, it is also known that the majority of respondents (53.47%) have income between 5 - 10 million.

Table 2. Demographic profile (n = 101)

Distribution by	Categories	Qty	Percentage
Gender	Male	58	57.43%
	Female	43	42.57%
Age	17 – 20 years old	12	11.88%
	21 – 25 years old	25	24.75%
	26 – 30 years old	50	49.50%
	31 – 35 years old	8	7.92%
	36 – 40 years old	5	4.95%
	41 – 45 years old	1	0.99%
Occupation	Student	5	4.95%
	Employee	84	83.17%
	Unemployed	4	3.96%
	Household	6	5.94%
	Teachers	2	1.98%
Education	High School	5	4.95%
	Undergraduate	89	88.12%
	Graduated	6	5.94%
	Doctoral	1	0.99%
Earnings	< 5 Million	5	4.95%
	5 – 10 Million	54	53.47%
	10 – 20 Million	39	38.61%
	20 – 30 Million	2	198%
	> 30 Million	1	0.99%

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4.2 Validity and Reliability Test

Validity and reliability tests are measured by calculating the value of CR to measure data consistency. To calculate the results of hypothesis testing from the collected responses, testing was carried out with the help of software namely SmartPLS, which is a statistical calculating device based on the partial least squared structural equation modeling (PLS-SEM) method. The following are the results of testing the validity and reliability of hypothesis testing.

Table 3. Result of Validity and Reliability Test

Variable	Code	Loading Factor	CR	Cronbach's Alpha	Status
Control Over Personal Information	CPI1	0.895	0.900	0.837	Valid
	CPI2	0.901			
	CPI3	0.782			
Use of Information	UIN1	0.777	0.903	0.824	Valid
	UIN2	0.828			
	UIN3	0.935			
Privacy Notes	PNT1	0.871	0.910	0.870	Valid
	PNT2	0.921			
	PNT3	0.893			
Information Disclosure	IDIS1	0.911	0.911	0.871	Valid
	IDIS2	0.936			
	IDIS3	0.905			

From Table 3, it can be seen that all variable's Loading factor are above 0.7, which can be indicated that all variables are valid. It also can be seen that the Composite Reliability and Cronbach's Alpha of all variables are above 0.7, this can be concluded that all variables are reliable.

4.3 Empirical Findings

From the results of hypothesis testing using Partial Least Square (PLS), it shows that all hypothesis can be accepted as follows:

Table 4. The Result of Hypothesis Testing

H	Standard Deviation	T-Statistic	P-Values	Status
H1	0.125	2.122	0.034	Supported
H2	0.123	2.478	0.013	Supported
H3	0.114	3.529	0.000	Supported

Note: Supported with $p \leq 0.05$, $t \geq 1.96$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

H1: Personal information disclosures on smartphone can be reduced by user's high control over personal information.

The effect of user's high control on personal information disclosures on smartphone gets 0.034 for p-value, which is smaller than 0.05. And gets 2.122 for t-statistics, which greater than 1.96. From these results, it can be concluded that hypothesis one (H1) "Personal information disclosures on smartphone can be reduced by user's high control over personal information" is accepted and supported by the data.

H2: When the user of smartphone has more information about the use of their personal information, they will disclose their personal information.

The effect of user's knowledge about the use of their personal information will disclose their personal information on smartphone gets 0.013 for p-value, which is smaller than 0.05. And gets 2.478 for t-statistics, which greater than 1.96. From these results, it can be concluded that hypothesis two (H2) "When the user of smartphone has more information about the use of their personal information, they will disclose their personal information" is accepted and supported by the data.

H3: The notification of privacy in smartphone usage increases the possibility of disclosing information/user data.

The effect notification of privacy in smartphone usage will increases the possibility of disclosing information/ user data gets 0.000 for p-value, which is smaller than 0.05. And gets 3.529 for t-statistics, which greater than 1.96. From these results, it can be concluded that hypothesis three (H3) "The notification of privacy in smartphone usage increased the possibility of disclosing information/ user data" is accepted and supported by the data.

5. DISCUSSIONS

The use of smartphones today that cannot be separated from people makes it a risk for its users. The more users depend on smartphone services, the higher the risk that users will face [11]. Various services in smartphones to increase the ease and practicality of users, open the opportunity for information disclosure to irresponsible parties. Detect user location, store personal data, store credit card details and allow users to access bank accounts are some examples of services that require users to disclose the information [13].

Actually, there is a contradiction between whether or not a user needs to disclose information on a mobile application or a mobile platform. If users intentionally disclose their personal information, user should face a risk of losing that information or being misused by others [13]. On the other hand, giving access to personal information aims to facilitate the activities of everyday smartphone users.

The result found in this study are in line with what was found in Benson's study. Benson found that the user's control over personal information had a negative relationship with information disclosure [1]. This is similar with what was found in this study. The higher user's control over personal information, the lower possibility of personal information disclosure.

In addition, other findings in this study showed the relationship between user awareness and security notices with information disclosure having a strong relationship. Similar like the results found by Benson that there was a positive relationship between user awareness with information disclosure and security notices with information disclosure [1]. While what was found in this study was the higher the level of user awareness or the more intense notices regarding security were given before disclosing personal information, the higher the possibility of the user to disclose their personal information.

5.1. LIMITATIONS AND FUTURE RESEARCH

As this research has few limitations, the results obtained are not optimal, therefore the subject needs further development in the future. The limitations we have are, first, we collected questionnaires with the total of the respondents are only 101. However, the questionnaires that can be processed collected meet the number of standard samples. Minimum number of samples that can be processed with SEM analysis technique are 100 to 500 samples (Ghazali, 2013). In the future, it is hoped that the samples researched are more than 500 respondents.

Second, the respondents of this research are the active users of smartphone from JABODETABEK (Jakarta, Bogor, Depok, Tangerang, Bekasi) area. In the future, in order to get better results, the research can be done with the respondents of the active users of smartphone from all over Indonesia. Based on the questionnaires collected, obtained demographic data of the respondents; included genders, ages, occupations, educations, dan salaries.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Third, we only use 3 variables in this study. To get better results, other variables must be added for future research, such as users' experiences or social influences that can affect users' decisions in disclosing their personal information.

Finally, this study was not discuss about the security on mobile devices or mobile platforms whether affecting disclosure of users' personal information or not, since according to [25] there are differences in security between 2 biggest mobile platform right now, Android and iOS.

6. CONCLUSION

This study aims to determine what factors influence smartphone users to disclose their personal information and provide access to mobile applications. Based on our finding, the results obtained are as in Table 5.

Table 5. Summary of Result

H	Hypothesis	Status
H1	Personal information disclosures on smartphone can be reduced by user's high control over personal information.	Supported
H2	When the user of smartphone has more information about the use of their personal information, they will disclose their personal information.	Supported
H3	The notification of privacy in smartphone usage increases the possibility of disclosing information/user data.	Supported

From the results of the analysis carried out, we found that control of over personal information, usage of information, and privacy notice was an influence factor for someone to disclose information.

We find that as long as the user knows the function of the disclosure information and gets privacy notifications, user will tend to disclose their personal information and give permission to third parties to access them. Meanwhile, personal information disclosures on smartphone can be reduced by user's high control over personal information.

REFERENCES

[1] V. Benson, G. Saridakis, and H. Tennakoon, "Information disclosure of social media users," *Inf. Technol. People*, vol. 28, no. 3, pp. 426–441, Aug. 2015.

[2] S. Conger, J. H. Pratt, and K. D. Loch, "Personal information privacy and emerging technologies," *Inf. Syst. J.*, vol. 23, no. 5, pp. 401–417, 2013.

[3] S. DMO, "Number of mobile phone internet users in Indonesia from 2015 to 2022 (in millions)," 2017.

[4] S. DMO, "Smartphone penetration rate as share of the population in Indonesia from 2015 to 2022*," 2017.

[5] S. DMO, "Share of population that use smartphones for online activities in Indonesia as of January 2018, by activity," 2018.

[6] T. Kontzer and L. Greenemeier, "Sad state of data Security," *InformationWeek*, vol. 1070, pp. 18–21, 2006.

[7] Tempo.co, "Indonesia's Cyber Security Awareness Still Low : Observer," 2015. .

[8] Kominfo.go.id, "Kominfo Imbau Kembangkan Budaya Cyber Security Awareness," 2016. [Online]. Available: https://www.kominfo.go.id/content/detail/7831/kominfo-imbau-kembangkan-budaya-cyber-security-awareness/0/berita_satker. [Accessed: 22-Jan-2019].

[9] R. Akraman, C. Candiwan, and Y. Priyadi, "Pengukuran Kesadaran Keamanan Informasi Dan Privasi Pada Pengguna Smartphone Android Di

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Indonesia," *J. Sist. Inf. BISNIS*, vol. 8, no. 2, p. 115, Oct. 2018.

[10] M. Amin, J. Penelitian, and P. Komunikasi, "Pengukuran Tingkat Kesadaran Keamanan Informasi Pengukuran Tingkat Kesadaran Keamanan Informasi Menggunakan Multiple Criteria Decision Analysis (MCDA) Information Security Awareness Level Measurement Using Multiple Criteria Decision Analysis (MCDA)," Juli-Oktober, 2014.

[11] H. Chan and D. S. Mubarak, "Information Security Awareness Levels of TAFE South Australia Employees University of South Australia," 2011.

[12] T. Line, J. Jain, and G. Lyons, "The role of ICTs in everyday mobile lives," *J. Transp. Geogr.*, vol. 19, no. 6, pp. 1490–1499, 2011.

[13] H. Zhu, H. Xiong, Y. Ge, and E. Chen, "Mobile app recommendations with security and privacy awareness," in *Proceedings of the 20th ACM SIGKDD international conference on Knowledge discovery and data mining - KDD '14*, 2014, pp. 951–960.

[14] I. A. Afandi, A. Kusyanti, and N. H. Wardani, "Analisis Hubungan Kesadaran Keamanan , Privasi Informasi , Perilaku Keamanan Pada Para Pengguna Media Sosial Line," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 1, no. 9, pp. 783–792, 2017.

[15] A. K. Jain and D. Shanbhag, "Addressing security and privacy risks in mobile applications," *IT Prof.*, vol. 14, no. 5, pp. 28–33, Sep. 2012.

[16] T. Dinev and P. Hart, "An extended privacy calculus model for e-commerce transactions," *Inf. Syst. Res.*, vol. 17, no. 1, pp. 61–80, 2006.

[17] M. A. Q. Vitale, "Control Over Personal Data, Privacy And Administrative Discretion In Europe And The Usa: The Paradox Of Italian 'Data Protection Authority,'" *John Marshall J. Inf. Technol. Priv. Law*, vol. 30, no. 4, pp. 720–756, 2014.

[18] M. Raento, A. Oulasvirta, R. Petit, and H. Toivonen, "ContextPhone: A Prototyping Platform for Context-Aware Mobile Applications," *IEEE Pervasive Comput.*, vol. 4, no. 2, pp. 51–59, Apr. 2005.

[19] M. Butler, "Android: Changing the mobile landscape," *IEEE Pervasive Comput.*, vol. 10, no. 1, pp. 4–7, 2011.

[20] H. N. Chua, A. Herbland, S. F. Wong, and Y. Chang, "Compliance to personal data protection principles: A study of how organizations frame privacy policy notices," *Telemat. Informatics*, vol. 34, no. 4, pp. 157–170, 2017.

[21] C. Callanan, B. Jerman-Blažič, and A. J. Blažič, "User awareness and tolerance of privacy abuse on mobile Internet: An exploratory study," *Telemat. Informatics*, vol. 33, no. 1, pp. 109–128, 2016.

[22] M. Sarstedt, C. M. Ringle, and J. F. Hair, "Partial Least Squares Structural Equation Modeling," in *Handbook of Market Research*, M. Christian Homburg, Ed. Cham: Springer International Publishing, 2017, pp. 1–40.

[23] K. Kwong-Kay Wong, "Partial Least Squares Structural Equation Modeling (PLS-SEM) Techniques Using SmartPLS," *Mark. Bull.*, vol. 24, no. 1, pp. 1–32, 2013.

[24] N. Kock, "Hypothesis Testing with Confidence Intervals and P Values in PLS-SEM," *Int. J. e-Collaboration*, vol. 12, no. 3, pp. 1–6, Jul. 2016.

[25] I. Mohamed and D. Patel, "Android vs iOS Security: A Comparative Study," *2015 12th Int. Conf. Inf. Technol. - New Gener.*, pp. 725–730, Apr. 2015.

Journal of Theoretical and Applied Information Technology
30th April 2019. Vol.97. No 8

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Annexure A

Questionnaire

A. Demographic Questions

1. What is your gender?

   ○ Male ○ Male

2. How old are you?

   ○ 17 - 20 ○ 21 - 25 ○ 26 - 30 ○ 31 - 35 ○ 36 - 40 ○ 41 - 45 ○ 46 - 50

3. What is your occupation?

   ○ Student ○ Employee ◉ Unemployeed ○ Household ○ Teacher

4. What is the highest level of education you have completed?

   ○ Highschool ○ Graduated ○ Undergraduated ○ Doctoral

5. What is your monthly income?

   ○ < 5 Million ○ 5 - 10 Million ○ 10 -20 Million ○ 20 - 30 Million ○ > 30 Million

B. Survey Questions

a) Control Over Personal Information		
1	I have control over my personal information, include whoever will get access to it by collecting them through mobile application and mobile platform (Google/ iOS)	○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree
2	I have control over how personal information is used	○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3	I can control my personal information which was provided to mobile application or mobile platform (Google/ iOS)	○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree
b) Use of Information		
4	The owner of personal information should give authorization for his/ her personal information before third parties (mobile application or mobile platform) can access to them	○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree
5	I forbid any third parties (mobile application/ mobile platform) sell my personal information which I have entrusted to them.	○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree
6	I forbid any third parties (mobile application/ mobile platform) share my personal information to other companies unless I have authorized it.	○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree
c) Privacy Notices		
7	Security features (e.g. SSL, HTTPS) are critical in your decision to allow permission to use data that have been submitted.	○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree
8	The content of privacy policy that've been provided by mobile platform (Google/ iOS) is important for me before I give any permission for data usage.	○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

9	The security seals of mobile platform (Google/ iOS) is important for me to give permission to the platform to use my submitted data	○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree
d) Information Disclosure		
10	I am willing to disclose personal information to third parties.	○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree
11	I am not worried if my personal information is revealed to trusted third parties	○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree
12	I have disclosed my personal information to trusted third parties	○ Strongly Disagree ○ Disagree ○ Neutral ○ Agree ○ Strongly Agree