Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 197 (2022) 576–582

Procedia Computer Science

www.elsevier.com/locate/procedia

Sixth Information Systems International Conference (ISICO 2021)

Investigating mobile users' intention: Technology acceptance and privacy perspectives

Ari Kusyanti[a,*], Nurudin Santoso[a], Harin Puspa Ayu Catherina[b], Evi Oktavia[b]

[a]*Department of Computer Science, Universitas Brawijaya, Malang, Indonesia*
[b]*Department of Information Systems,Universitas Brawijaya, Malang,Indonesia*

Abstract

Smartphones are essential devices in most people's lives nowadays. There are many benefits offered by smartphones, such as: the ability to access the internet, e-mail, access social media, etc. Their advanced features and ease of use enhances their functionality including storing contacts, photos, videos and other sensitive information. Thus, smartphones become attractive target for hackers especially with regard to get unauthorized access to sensitive data from users that violates their privacy. This paper investigated the impact of users' intention in using a smartphone despite privacy threats that can occur. Questionnaires were distributed to 300 respondents who were actively using a smartphone to obtain the study data. The level of relationships among the constructs were analysed using Structural Equation Modelling (SEM). The results of this study indicate that the factors that influence users in using a smartphone are mobile users' information privacy concern, perceived ease of use and perceived usefulness.

Keywords: Smartphone; mobile users' information privacy concern; mobile user intention; TAM; SEM.

1. Introduction

Smartphone has long played an important part in the global growth of telecommunication media. Technological advancements make smartphones more popular and become one of the most advanced communication tools. In 2020, a report from Statista indicated that the total of active smartphone users in Indonesia is 191.6 million users [1]. Thus, Indonesia is a country with the fourth most populated active smartphone users in the world following China, India and

* Corresponding author. Tel.: +62-341-577-911; fax: +62-341-577-911.
E-mail address: ari.kusyanti@ub.ac.id

1877-0509
10.1016/j.procs.2021.12.175

United States [2].

Today, smartphones are beginning to shift the use of personal computers as their sophisticated features and functionality. There are many benefits offered by smartphones, such as: the ability to access the internet, e-mail, access social media, and many other benefits. With the increasing popularity of smartphone, privacy has become a major concern for users because many applications on smartphones collect and share sensitive data from users [3]. Therefore, smartphones are attractive target for hackers especially with regard to the many ways to install malicious code remotely on their victims and violating access to important data. An article on the Wall Street Journal website mentions that Apple iOS and Google Android collect smartphone user information through locations and periodically build a large database, and in some cases, it was found that the database might be connected to third parties without the knowledge of smartphone users [4]. According to Kapersky, as many as 20,000 Android-based smartphones of various types and brands have vulnerabilities in the critical category as of 87.7% worldwide [5]. In 2018 there was an article published on the Wall Street Journal website which stated that there are Android-based smartphones that secretly collect data in the form of: IMEI, MAC Address and device location from the user and then send the data to the server and sell the data to an advertising company [6].

The number of cases that occur involving the use of smartphones prove that not always the smartphone brings positive benefits to its users. However, according to study conducted by Mylonas et al., [7] reveals that security and privacy awareness of smartphone users is still lacking. Furthermore, based on their research, most of smartphone users are concerns about their privacy when using a smartphone, but they still carry out risky behavior.

This study responds to recent call to investigate what factors influence users' intention in using a smartphone despite privacy threats that can occur using the Mobile User's Information Privacy Concerns (MUIPC) and Technology Acceptance Model (TAM) models. The Mobile User's Information Privacy Concerns (MUIPC) model is adapted from a study conducted by Xu et al. [8] While the Technology Acceptance Model (TAM) model is adapted from the research conducted by Joo et al. [9]. The rest of the paper discuss the relevant literature review, methodology, discussion, and conclusion sections.

2. Theoretical Framework and Hypothesis

2.1. Mobile Users' Information Privacy Concern (MUIPC)

Mobile information privacy concern (MUIPC) is a theory used to explore interactions between mobile users and service providers related to privacy issues [8]. Mobile User Information Privacy Concern (MUIPC) also states that personal information from users can be used for information exchange by smartphone vendors. However, the fact is that these users do not know clearly about the privacy policy of the information they have disclosed [8].

Perceived Surveillance is defined as the extent to which an individual can supervise personal data and personal activities contained on his smartphone that can be seen, heard or monitored by other parties [8]. An individual often has the perception that he does not like that his personal data are collected by other parties in large numbers. As mentioned in [10], Perceived Intrusion is defined as the extent to which a disturbance can cause discomfort, danger and need protection even if the information is barely disseminated [10]. Secondary Use of Information is defined as a phenomenon where personal information is collected from a person for a certain purpose but is misused without the permission of that person [11]. The activity of using secondary information can potentially generate fear and uncertainty about how personal information from an individual will be used in the future and can cause vulnerability [10].

2.2. Technology Acceptance Model (TAM)

Technology Acceptance Model (TAM) [12] is a theory to examine user acceptance of information systems that aims to provide an explanation of the acceptance of user's behavior towards various types of technology. Technology Acceptance Model (TAM) can not only predict, but also provide an explanation so that when a system is declared unacceptable to the user, then the explanation can be used to determine the steps that must be taken next. In particular, there are three dimensions used in the Technology Acceptance Model (TAM), namely: Behavioral Intention, Perceived Usefulness and Perceived Ease of Use.

2.3. Prior Privacy Experience

Prior Privacy Experience is defined as the individual's level previous experience relates to the handling of privacy issues previously experienced [11]. Xu et al. [8] stated that when mobile users experienced data misused previously

or heard about news regarding privacy violation, they tend to have stronger information privacy concerns.

2.4. Hypotheses Development

In the theory of Mobile User Information Privacy Concern (MUIPC) there are 3 dimensions to measure understanding between smartphone users and service providers related to privacy issues, namely: Perceived Surveillance, Perceived Intrusion and Secondary Use of Information. Malhotra et al. [13] stated that data collection conducted by third parties whether legitimate or illegitimate is the beginning of various kinds of privacy problems. At present, more and more data collection activities are carried out by mobile applications, operating systems that induce intensive data recording and the impression that vendors are constantly monitoring user behavior through smartphones. In today's mobile environment, vendors utilize powerful technology to track and monitor profiles of users [8]. Smartphone users can reject mobile applications if they are afraid that their personal activities can be monitored, recorded and transmitted to various entities [8]. Users will tend to be aware that their personal information or personal activities are monitored when they have experiences or events that have been experienced before related to the misuse of personal information on their smartphone. In related literature, intrusion is defined as an invasive action that disturbs the peace of a person [10]. It is said that instructors can interfere with activities or routines of victims and often make victims feel uncomfortable [10]. The main point that occurs is that the instructor can create discomfort and danger, so it requires limits and control in controlling the flow of personal information that has been given in order to restore the comfort level of the user [8]. Users who think that privacy is important and have prior experience related to misuse of personal information will feel the interference caused if they provide personal information to the public space and later it can cause privacy problems.

In practice, secondary use of personal information has the probability to threaten an individual's ability to maintain access to personal information and can endanger the individual [14]. Users who think that they have a high level of vulnerability and have prior experience related to misuse of personal information will tend to feel concerned about the control flow of personal information on their smartphones. Hence, the hypothesis is shown as follows:

H1: Prior privacy experience has a significant effect on mobile users' information privacy concern

In the previous literature of Mobile User's Information Privacy Concern (MUIPC) there are 3 dimensions used, namely: Perceived Surveillance, Perceived Instrusion and Secondary Use of Information. Users who have a high level of awareness and understanding of privacy tend to keep their privacy issues [15]. Users who feel that a technology has supervised, recorded and collected their personal information but they can feel the benefits provided by the technology, these users will tend to have the intention to continue using the technology. In the study conducted by Solove [10] found that perceived intrusion can be an attack that is harmful to an individual's information space, which can be said to be the most important factor in privacy issues. However, users will tend to have the intention to continue using a technology even though there are disruptions that could potentially abuse their personal information when they assume that the technology can improve their performance. Culnan and Armstrong [16] also argue that users' are less-guarded towards privacy of information disclosure once they are able to control the use of personal information they have provided in the future. From this statement, the hypothesis drawn as follows:

H2: Mobile users' information privacy concern has a significant impact on behavioral intention

According to [12] ease of use refers to an individual's level belief that using a particular system can be very easy [12]. If an individual feel that if an application to be used is simple, easy to use and does not require much effort to use it, it will be considered that the application will provide many benefits [17]. Hence, the following hypothesis is proposed:

H3: Perceived ease of use has a significant effect on perceived usefulness

In a study conducted by Willis [18], it suggested that easy-to-use technology seemed to be easier to use than technology that is difficult to use, regardless of how useful the technology is. For this reason, it can be expected that there will be a direct and positive effect of the perceived ease of use at the intended use. Based on the discussion the following hypothesis is developed:

H4: Perceived ease of use has a significant impact on behavioral intention

Perceived usefulness is defined as an individual's level belief that using a particular system will improve performance in his work [12]. Users who feel that a technology can provide benefits and can improve their performance will tend to have the intention to continue using the technology. According to the review above, it can be drawn hypothesis as follows:

H5: Perceived usefulness has a significant effect on behavioral intention

Based on the hypothesis that has been defined above, Fig. 1 depicts the research model used.

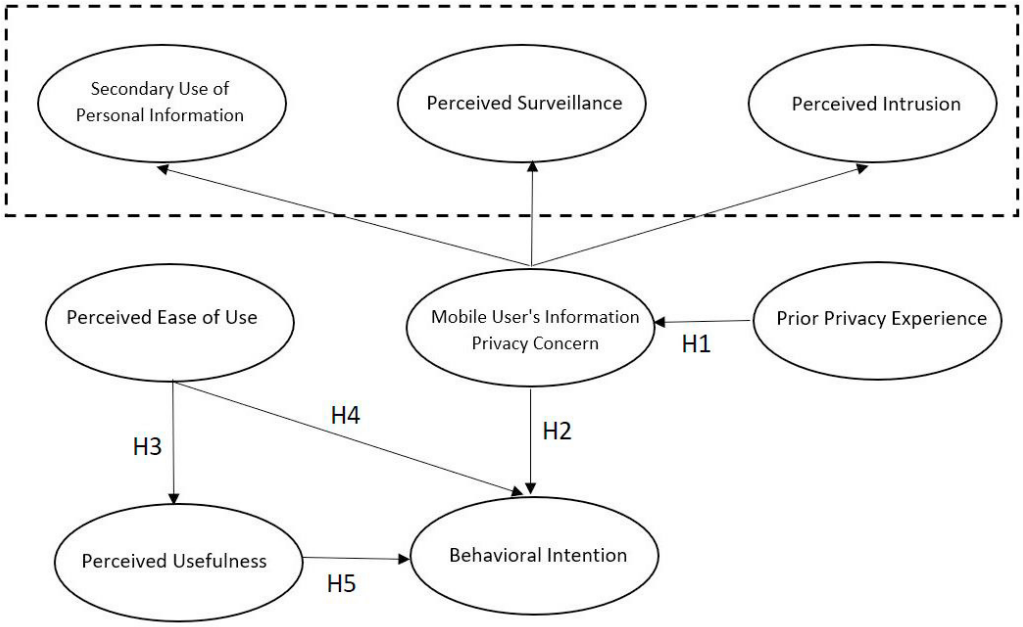

Fig 1. Research model

3. Research Method

3.1. Measurement Development

Data was collected from 300 respondents who acted as active smartphone users. The data is obtained using an online questionnaire around December 2020 from randomly selected university students in Indonesia. The survey questionnaire is divided in two main parts. In the first part, the respondents had to fill in demographic data, such as name, age, gender, education and occupation. Later, the respondents were asked to answer questions on a wide variety of items in accordance with MUIPC [8] and TAM [12] model. The instrument was scaled using seven-point Likert scale items, ranging from 1: Strongly Disagree to 7: Perfectly Agree. The survey questionnaire was built on the basis of previously validated instrument.

3.2. Survey Design

Beforehand, pilot study is carried out to ensure the validity of the instrument and that the survey questionnaire is not ambiguous. Cronbach's α is used, in which for all constructs have to be over 0.6 [19]. Table 1 displays the Cronbach's α of all variables which are above 0.6, and the overall Cronbach's α is 0.9, hence the internal consistency among item and the scale system is highly reliable. Another test is KMO with all variables are above 0.855 and Bartlett's test with the significant level is less than 0.05, thus the factor analysis method is can be applied to the

questionnaire [20].

Table 1. Cronbach's Alpha Value

Factors	Value
Prior Privacy Experience (PPE)	0.657
Perceived Ease of Use (PEU)	0.906
Perceived Usefulness (PU)	0.833
Behavioral Intention (BI)	0.804
Mobile User Information Privacy Concern (MUIPC)	
- Secondary Use of Personal Information	0.726
- Perceived Surveillance	0.755
- Perceived Intrusion	0.842

4. Data Analysis

4.1. Measurement Model Fit

All of the items of the scale were subjected to further test i.e. Confirmatory Factor Analysis (CFA) to determine how precisely indicators explains construct variables that already exist. These results are used to validate the uni-dimensionality of measurement model. The results of fit model resented in Table 2.

Table 2. Goodness of Fit Index

Index	Criteria	Value	Info
Chi-square	>0.05	1542.247	Good
CMIN/DF	1.00 < CMIN/DF < 3.00	2.470	Good
GFI	>0.9	0.9062	Good Fit
RMSEA	<0.05 good fit	0.044	Good Fit

4.2. Structural Model Fit

After the measurement model was validated, structural fit models using Path Analysis is continued. Structural fit models are used to analyze the relationship between variables in the research model [21]. Table 3. presents the significance p-values for every path in the model. The results show that H1 ($p = 0.0034$) is accepted which can be interpreted that Prior Privacy Experience plays significant role towards Mobile Users' Information Privacy Concern. H2 is accepted ($p= .002$) that highlights a significant relationship between Mobile Users' Information Privacy Concern towards Behavioral Intention. H3 is rejected ($p = 0.436$) which postulate that Perceived Ease of Use does not relate to Perceived Usefulness. H4 and H5 are both accepted with =*** and 0.011) that support the notion that Perceived Ease of Use and Perceived Usefulness influence the Behavioral Intention.

Table 3. Structural Model Fit Result

Hypothesis	p-value (<0.05)	Info
MUIPC ← PPE	.0034	Accepted
BI ← MUIPC	.002	Accepted
PU← PEU	.436	Rejected
BI ← PEU	***	Accepted
BI ← PU	.011	Accepted

5. Result and Discussion

The study is seeking to establish an integration between TAM and MUIPC model towards Behavioral Intention of smartphone users. Based on the results, four hypotheses out of the five hypotheses proposed have been supported. In TAM model, Perceived Ease of Use and Perceived Usefulness influence the Behavioral Intention. Respondents assume that interacting with smartphone that they normally use is easy. Respondents also thought that to use smartphone features does not require much effort. In addition, it was easy to learn hence they intend to use the smartphone. This shows that the study of perceived ease of use (PEU) has a significant effect on behavioral intention (BI). The results of this study are affirmed by Willis [18] which suggests that when the use of technology is an easy to use thing it will make an individual will have the tendency to continue using the application. At the same time, respondents assume that when they decided to use a smartphone to support their activities, they can improve their effectiveness and performance in supporting their activities or work. Respondents also thought that through the use of smartphones they got the information they need. This shows that in this study perceived usefulness (PU) has a significant effect on behavioral intention (BI). As mentioned in Venkatesh, Morris and Ackerman [23] suggesting that if an individual uses an application and the individual think that the application can provide benefits and can improve his performance at work, then the individual will tend to have intentions to continue using the application. However, Perceived Ease of Use does not relate to Perceived Usefulness which indicates that when respondents learn how to use smartphones, they tend to find it difficult to use several applications. Also, when they interacted with their smartphone continuously, it required a lot of effort. So that respondents tend to not be able to get the benefits of smartphone. This shows that the study of perceived ease of use (PEU) has no significant effect on perceived usefulness (PU). Study by Praveena and Thomas [22] supported the result when a technology is difficult to use by its users and does not provide complete guidance for its users, these users will tend to not be able to get the benefits of the technology.

As for MUIPC model, Mobile Users' Information Privacy Concern itself shows significant relationship towards Behavioral Intention shown significant relationship. Respondents consider that they are aware of privacy i.e. misuse of personal information and the impact of providing personal information and can handle it when their personal information is misused. Respondents also assumed that when they were aware of the importance of safeguarding their privacy, they could reduce the impact of misuse of their personal information. Thus, respondents intend to continue using smartphones, because they already have an awareness of privacy issues. This shows that in this study mobile users' information privacy concern (MUIPC) has a significant effect on behavioral intention (BI). Malhotra [13] confirmed that understanding privacy is the basis for an individual to use an application, when they feel that the application is safe and they have knowledge of privacy issues they will tend to minimize the occurrence of privacy abuse hence they continue to use the application. Additionally, Prior Privacy Experience plays significant role towards Mobile Users' Information privacy concern. Respondents whom experienced misuse of personal information due to collection of personal information by vendors and carried out without their consent, they are tend to be more concern towards privacy. This shows this study of prior privacy experience (PPE) has a significant effect on mobile users' information privacy concern (MUIPC). Similarly, Xu et al. [8] who argued that when someone considers privacy to be important to him and has had an experience of misuse of privacy before, it will make respondents continue to follow and understand the importance of privacy and its impact if they provide personal information on certain technologies.

6. Conclusion

This study presents complete results from various aspects such as reliability and validity, path analysis, factor analysis, to perform Structural Equation Modeling (SEM) to perform an empirical analysis on questionnaire regarding the factors that influence the intention of users in using smartphones by integrating TAM and MUIPC model, namely: mobile users' information privacy concern, perceived ease of use and perceived usefulness. Respondents thought that to operate features of smartphone did not require much effort. Respondents also assumed that many benefits were obtained when they used smartphones and this could improve their performance. However, respondents assume that they have a high level of knowledge about privacy so they tend to understand more about the misuse of personal information and the impact of providing personal information. This empirical study sheds light on studies users'

intention to realize the importance of mobile users' privacy concerns. However, our study is subject to limitation. Since the study was conducted with respondents from Indonesia, a survey in other countries may lead to different results. Hence, it is very interesting to compare the result from countries with different privacy perception.

References

[1] Statista. (2021) "Number of smartphone users in Indonesia from 2015 to 2025." https://www.statista.com/statistics/266729/smartphone-users-in-indonesia/

[2] Statista. (2021) "Number of smartphone users by leading countries as of May 2021." https://www.statista.com/statistics/748053/worldwide-top-countries-smartphone-users/

[3] Egelman, S., A. P. Felt, and D. Wagner. (2013) "Choice architecture and smartphone privacy: There's a price for that." in R. Bohme (eds.), *The economics of information security and privacy*. Berlin, Heidelberg.

[4] Angwin, Julia, and Jennifer Valentino-Devris. (2011). "Apple, Google Collect User Data." https://www.wsj.com/articles/SB10001424052748703983704576277101723453610

[5] Ayyubi, Al Sholahuddin. (2015) "Alert! Android Phones Vulnerable to Theft." http://industri.bisnis.com/read/20151025/105/485772/waspada-ponsel-android-rentan-pencurian-data.

[6] Noviadhista, U.F. (2018) "Revealed, This Android Smartphone Steals User Data!." https://technologue.id/terungkap-smartphone-android-ini-curi-data-data-penggunanya/amp/.

[7] Mylonas, A., A. Kastania, and D. Gritzalis. (2015) "Delegate the smartphone user? Security awareness in smartphone platforms." *Internet Security Threat Report*. Symantec.

[8] Xu, Heng, Sumeet Gupta, Mary Beth Rosson, and John M. Carroll. (2012) "Measuring Mobile Users Concerns for Information Privacy." *Thirty Third International Conference on Information Systems Orlando.*

[9] Joo, J., and Y. Sang. (2013) "Exploring Koreans' smartphone usage: An integrated model of the technology acceptance model and uses and gratifications theory." *Computers in Human Behavior* **29** (2013): 2512–2518.

[10] Solove, D.J. (2006) "A Taxonomy of Privacy." *University of Pennsylvania Law Review* **154** (3): 477-560.

[11] Smith, H.J., J.S. Milberg, and J.S. Burke. (1996) "Information Privacy: Measuring Individuals' Concerns About Organizational Practices." *MIS Quarterly* **20** (2): 167-196.

[12] Venkatesh, Viswanath, and Fred D. Davis. (2000) "A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies." *Management Science* **46** (2): 186-204.

[13] Malhotra, Naresh K., Sung S. Kim, and James Agarwal. (2004) "Internet users's information privacy concerns (IUIPC): The construct, the scale, and a causal model." *Information systems research* **15**(4): 336-355.

[14] Culnan, Mary J., and Cynthia Clark Williams. (2009) "How Ethics Can Enhance Organizational Privacy: Lessons from the Choicepoint and Tjx Data Breaches." *MIS Quarterly* **33** (4): 673-687.

[15] Dinev, Tamara, and Paul Hart. (2006) "An Extended Privacy Calculus Model for E-Commerce Transactions." *Information Systems Research* **17**(1): 61-80.

[16] Culnan, Mary J., and Pamela K. Armstrong. (1999) "Information Privacy Concerns, Procedural Fairness and Impersonal Trust: An Empirical Investigation." *Organization Science* **10** (1): 104-115.

[17] Tan, Xin, Li Qin, Yongbeom Kim, and Jeffrey Hsu. (2011) "Impact of Privacy Concerns in Social Networking Web Sites." Internet Research **22** (2): 211-233.

[18] Willis, T. (2008) "An evaluation of the technology acceptance model as a means of understanding online social networking behavior." *Theses and Dissertations, Paper* 568.

[19] Malhotra, K.N. (2007) "Marketing Research an Applied Orientation. International Edition." Pearson.

[20] Field, A. (2009) "Discovering statistics using spss." 3rd ed. Sage Publications.

[21] Hair, J. F., William C. Black, B. J. Babin, R. E. Anderson, and R. L. Tatham. (2010) "Multivariate Data Analysis, Seventh Edition." Pearson Prentice Hall.

[22] Praveena, K., and S. Thomas. (2013) "Continuance Intention to Use Facebook: Role of Perceived Enjoyment and Trust." *The International Journal Of Business & Management*.

[23] Venkatesh, Viswanath, Fred Davis, and Michael G. Morris. (2007) "Dead or alive? The development, trajectory and future of technology adoption research." *Journal of the Association for Information System Vol. 8 No.4*