Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 00 (2018) 000–000

Procedia Computer Science

www.elsevier.com/locate/procedia

4th Information Systems International Conference 2017, ISICO 2017, 6-8 November 2017, Bali, Indonesia

Information Privacy Concerns on Teens as Facebook Users in Indonesia

Ari Kusyanti, Dita Rahma Puspitasari, Harin Puspa Ayu Catherina, Yustiyana April Lia Sari

Faculty of Computer Science, Universitas Brawijaya

Abstract

Facebook is the most popular social media among teens. In a research conducted by Crowd DNA to 13 countries, two-third of teens aged 13-24 checking on their Facebook 14 times a day. Along with the rising of social media development and popularity, issue of privacy concerns has become public attention. This paper attempted to investigate Facebook users' information privacy concerns using Internet Users' Information Privacy Concerns (IUIPC). The data used in this research is collected from a questionnaire survey and analyzed using Structural Equation Modelling (SEM). The result shows that although users are aware with the risk of information loss by using Facebook, it does not have effect on their intention to use Facebook.

Peer-review under responsibility of the scientific committee of the 4th Information Systems International Conference 2017.

Keywords: Social Media; Teens; Privacy; IUIPC; SEM

1. Introduction

Facebook is a social media founded by Mark Zuckerberg in 2004 for people in Harvard University. From September 2005 people outside Harvard starting to be able to access Facebook [1]. Facebook Press Room stated that in 2010 Facebook had 400 million active users from all over the world [2]. Previous research shows that Facebook is the most used social media by teens [3]. A research conducted by Crowd DNA shows that teens are checking on their

* Corresponding author. Tel.: +62-81-233-799-049 ; fax: +62-341-577-911 .
E-mail address: ari.kusyanti@ub.ac.id

Peer-review under responsibility of the scientific committee of the 4th Information Systems International Conference 2017.

Facebook account 14 times a day and another research conducted by JakPat shows that 80.9% teens aged from 16-19 in Indonesia are accessing their Facebook account every week [4] [5]. Their online activities including sharing posts, updating profile, uploading videos and pictures etc.

Based on several surveys conducted among Internet users worldwide, the awareness of digital foot print of their online activities from different age groups are increasing [6]. The most important concern for Internet users is that their personal information might be accessed, exchanged and manipulated without their concern. Hence, it is highly recommended that personal information of Internet users should be handled with respect to their privacy. In pursuance of indicating how the privacy for internet users can be secured and the security of their personal information can be assured, it is important to embrace the concerns of internet users in relation to their information privacy.

There is a regulation which protects kids under 13 from an organization which collecting personal information. However, teens above 13 who will voluntary give their personal information with a little awareness about risk rarely discussed [7]. In addition, existing research on privacy concerns mostly concentrated on the United States [8]. Instead of comparing to the United States, this research focuses on privacy issues that concern Internet users from Indonesia, where cultural, social, demographic and enviroumental factors are different from the United States.

This research uses Information Users' Privacy Concerns (IUIPC) which proposed by [9] to investigate teens' privacy awareness in using Facebook. Data are collected through a questionnaire survey and analyzed by Structural Equation Modelling (SEM) to evaluate the hypotheses.

2. Model and hypotheses

There are several studies in information systems literature regarding privacy concerns. Two theoretical frameworks that are usually used are Concerns for Information Privacy (CFIP), and Internet Users' Information Privacy Concerns (IUIPC) [8]. The former has been the first theoretical framework for measuring privacy concerns that have gained wide researcher attention [10]. According to [10], CFIP is an empirical quantitative methodology for measuring privacy concerns of a user in online environments in a multidimensional scale. This scale has been applied in determining user's concerns about organizational information privacy practices [9]. The dimensions of CFIP are collection, unauthorized secondary use, improper access, and errors.

The later have been developed by Malhotra et.al. A construct of Internet Users' Information Privacy Concerns which consists of three main dimensions of control, awareness, and collection, which are specified as a scalar variable. Furthermore, Malhotra et al. have developed a model by integrating the Internet Users Information Privacy Concerns (IUIPC) theory as the first order theoretical framework with Trust concept [11]. Trust is considered as an important motive to justify users' behavior in sharing their information online, when there is a risk of violating their privacy. In other words, users' behavior tends to be influenced by trust in a risky environment.

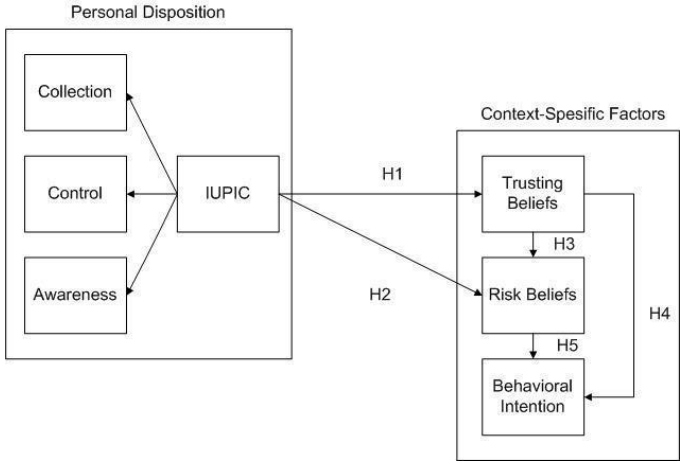

Fig. 1 Internet Users' Information Privacy Concerns model

This research uses a model proposed by [9], Internet Users' Information Privacy Concerns (IUIPC) to investigate teens' information privacy concerns regarding their usage on Facebook. IUIPC is a model to reflect internet users' attention towards information privacy. The difference between this study and prior study lies in the object of study. Prior study uses internet in general and this research focuses on Facebook as a social media. The model of IUIPC is shown in Fig. 1.

2.1. Definition of each construct

Based on the model previously described, the definition of each constructs that used in this research is presented in Table 1.

Table 1. Definition of each construct

Item		Definition	Reference
IUIPC	Collection	The degree to which people are aware about the activities of Facebook in collecting their personal information.	[9]
	Control	The freedom of people which determine whether he or she will give their personal information to Facebook.	
	Awareness	The degree to which people are aware about the activities of Facebook towards their personal information they have given.	
Trusting beliefs		The degree to which people believe wether Facebook is trustworthy in protecting users' personal information	
Risk beliefs		The degree to which people are aware about risk or high potential loss when disclosing their personal information to Facebook.	
Behavioural intention		An individual's intention in using Facebook.	

2.2. Hypotheses for the constructs

Users with a high degree of information privacy concerns are likely does not trust Facebook and concerning the risk that may occur [9].

H1: IUIPC have a negative effect on trusting beliefs.
H2: IUIPC have a positive effect on risk beliefs.

Previous research show that trust had a negative effect toward users' risk perception. The more they trust Facebook, the less likely they see the risk in providing their personal information to Facebook [9].

H3: Trusting beliefs have a negative effect on risk beliefs.

Previous research shows that trust and risk had direct effect on users' intention to do something. Trust would directly affect intention and that risk affects users' intention to buy something online [9].

H4: Trusting beliefs have a positive effect on intention to give personal information.
H5: Risk beliefs have a negative effect on intention to give personal information.

3. Data Analysis

The respondents of this study are high-school teens with the age range from 15 to 18. The data was collected through paper-based questionnaire survey and was distributed in a public senior high-school in Indonesia. The data are taken on Mid November – December 2016.

3.1. Descriptive analysis

Pilot study was conducted before the full-scale study to measure the reliability of each construct. Reliability was conducted to determine the respondent's consistency in answering the questionnaire [12]. Reliability was measured using Cronbach's alpha coefficient. The reliability of each construct is shown in Table 2.

Table 2. Construct reliability

Construct	Cronbach's α
	Criteria α > 0.6
Control (CTRL)	0.843
Awareness (AW)	0.860
Collection (CL)	0.902
Trust	0.812
Risk	0.842
Intention to Give Information (IGI)	0.608

A total of 303 questionnaires were collected. From all of the collected questionnaires, there are 294 valid response with response rate 97,03%. The characteristic of respondents is shown in Table 3.

Table 3. Characteristic of respondents

Age	Sample Size	%	Sex	Sample Size	%
15	72	24.49	Female	53	18.03
			Male	19	6.48
16	158	53.74	Female	115	39.12
			Male	43	14.63
17	57	19.39	Female	35	11.9
			Male	22	7.48
18	7	2.38	Female	4	1.36
			Male	3	1.02
Total	294	100		294	100

To ensure that there are no missing values in the collected data, Little's MCAR test was conducted. The result shows that there are no missing values. Mahalanobis distance value was calculated to determine the outlier. The mahalanobis distance 36.19 and the data that exceed this value is called outlier. There are 21 outliers and they are discarded.

3.2. Sample adequacy test

Kaiser-Meyer-Olkin test was used to measure the sampling adequacy to indicate whether factor analysis for the data sample is appropriate or not [13]. The KMO test result is 0.813 which categorize as great [13]. The criteria of KMO value is shown in Table 4.

3.3. Normality test

Normality test was conducted to determine whether the data sample is normally distributed or not. Kolmogorov-Smirnov test was used to calculate the normality of the data. The result of this test shows 0.01 which means the sample

is significantly different from normal distribution [13]. To avoid problems in further analysis, bootstrapping was conducted to automatically choose the normal data in the measurement model fit.

Table 4. KMO value criteria

Value	Criteria	Reference
<0.5	Not acceptable	[13]
0.5 – 0.7	Mediocre	
0.7 – 0.8	Good	
0.8 – 0.9	Great	
>0.9	Superb	

3.4. Measurement model fit

Measurement model fit was conducted to determine the compatibility between each indicator and its construct [12]. In measurement model fit, Confirmatory Factor Analysis is used [13]. The result of goodness of fit indices test shows that the model fitted to the data. The result is shown in Table 5.

Table 5. Goodness-of-fit indices

Fit index	Value	Recommended value	Reference
x^2/df	2.764	<3	[14]
GFI	0.881	>0.8	
AGFI	0.840	>0.8	
RMSEA	0.078	<0.08	
CFI	0.920	>0.9	

3.5. Hypotheses testing

Path analysis was conducted to evaluate the proposed hypotheses and to determine the relationship between construct in the model. The proposed hypotheses could be stated as supported if the relationship between its construct has significant value (t-value>1.96; p-value<0.05). The hypotheses testing result is shown in Table 6.

Table 6. Hypotheses testing result

Hypotheses	Relationships	t-value	p-value	Supported
Criteria		>1.96	<0.05* <0.01** <0.001***	
H1	IUIPC → TRUST	5.114	***	NO
H2	IUIPC → RISK	5.140	***	YES
H3	TRUST → RISK	-3.443	***	YES
H4	TRUST → IGI	5.846	***	YES
H5	RISK → IGI	-1.445	0.148	NO

4. Research and discussion

This paper attempted to analyze Facebook users with the age range from 15 to 18 years old about their reactions to various privacy threats may happen when they use Facebook. An IUIPC model was used to investigate it. IUIPC is a model consists of IUIPC itself as a second-order factor consists of three first-order dimensions—collection, control,

and awareness—and three other constructs—risk beliefs, trust beliefs, and behavioral intention. The data used in this research was collected through a questionnaire survey on a public senior high-school in Indonesia around mid-November – December 2016. The result of this research shows that there are two out of five hypotheses are unsupported.

- *H1 result discussion*
  Hypothesis 1 was rejected. Based on the result of Hypothesis 1 can be concluded that respondents regard their awareness of their information privacy in Facebook does not reduce their trust in Facebook. This may happen because they assume that Facebook will be consistent and honest with regard to the privacy of the information they have provided. This is due to social networking sites tell their users that they will do their best to protect users' personal information but do not guarantee that the third organization associated with them can be trusted as stated in their privacy policy. This research finding is in line with [15] that stated users of an application tend to ignore the privacy of information that may occur when they provide personal information to an application when they have a belief that the application will not misuse the personal information already provided.

- *H2 result discussion*
  Hypothesis 2 was accepted. Based on the result of Hypothesis 2, the finding of this research shows that respondents assume if their personal information that has been given to Facebook can be misused by other parties. In addition, respondents also assume that when they provide their personal information to Facebook it will be causing risks, such as: personal information they have provided may be misused by others. The result of [15] supports this research finding that described if an individual gives their personal information to the public does not guareantee the possibility of risks that may cause problems to their privacy.

- *H3 result discussion*
  Hypothesis 3 was accepted. Based on the result of Hypothesis 3, it can be concluded that the respondents assume that Facebook is a social media that can be trusted because the services that had been provided by Facebook will keep respondents' data safely and reliably to protect the privacy of users. Thus, they are less likely complaining despite the risks taken when providing personal information on Facebook. The risks including personal information may be misused, loss of privacy regarding providing personal information, etc. This research finding is in line with [15] that stated the more users believe in social media, the less the user fears the risks.

- *H4 result discussion*
  Hypothesis 4 was accepted. Based on the result of Hypothesis 4, it can be concluded that respondents assume that Facebook is a social media that can be trusted. Respondents believe that Facebook will not abuse the personal information that the respondents had provided. In addition, respondents also assume that Facebook will always be honest with regards to the use of the personal information they have provided. Therefore, the respondents have the intention to continue using Facebook. The result of [16] supports this research finding which stated that the more users believe in an application the greater the intention of the user to keep using the application.

- *H5 result discussion*
  Hypothesis 5 was rejected. Based on the result of Hypothesis 5 it can be concluded that respondents assume that although there will be risks caused by providing their personal information to Faecbook does not reduce the intention of these respondents to use Facebook. When these respondents can see the benefits and ease of using Facebook they will tend to ignore the risks that may occur. The result of [17] supports this research finding which explained that when an individual has an intention in using an app they will tend not to think about the risks that can occur.

5. Conclusion

The main purpose of this study is to investigate the Internet users' privacy concerns in the context of teen's behaviour in using Facebook as the demographic profile of the research in Indonesia. Our finding shows that although users are aware with the risk of information loss by using Facebook, it does not have affect on their intention to use Facebook.

The result may vary if the data was collected from different geographic background. Thus, on the basis of this research it is possible to confirm that the concept of Internet Users' Information Privacy Concerns can be applied in social media, such as Facebook. More investigation may be required like adding some constructs from different model to obtain a better understanding on information privacy issues regarding social media.

References

[1] Boyd, D.M. and Ellison, N.B. 2007. Social Network Sites: Definition, History, and Scholarship. Journal of Computer-Mediated Communication, 13(1), p.210-230 (http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2007.00393.x/epdf)

[2] Steinfield, C., Ellison, N., Lampe, C. and Vitak, J., 2012. Online Social Network Sites and the Concept of Social Capital. Frontiers in new media reasearch, 15, p.115-131 (https://msu.edu/~steinfie/Steinfield_Internetat40.pdf)

[3] Lenhart, A. 2015. Teens, Social Media & Technology Overview 2015. Pew Research Center Internet, Science & Tech (http://www.pewinternet.org/2015/04/09/teens-social-media-technology-2015/)

[4] Crowd DNA. 2014. Coming of Age on Screens. [online] Facebook IQ (http://www.pewinternet.org/2015/04/09/teens-social-media-technology-2015/)

[5] Emarketer. 2016. Facebook Remains the Largest Social Network in Most Major Markets. Emarketer (http://www.emarketer.com/Article/Facebook-Remains-Largest-Social-Network-Most-Major-Markets/1013798)

[6] Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. Journal of Consumer Affairs, 43(3), 389-418.

[7] Feng, Y. and Xie, W. 2014. Teens' Concern for Privacy When Using Social Networking Sites: An Analysis of Socialization Agents and Relationships with Privacy-protecting Behaviors. Computers in Human Behavior, 33, p.153-162 (http://www.sciencedirect.com/science/article/pii/S0747563214000144)

[8] Bélanger, F., and Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. MIS Quarterly, 35(4), 1017-1042.

[9] Malhotra, N.K., Kim, S.S. and Agarwal, J. 2004. Internet users's information privacy concerns (IUIPC): The construct, the scale, and a causal model. Information systems research, 15(4), p.336-355 (http://csis.pace.edu/ctappert/dps/d861-09/team2-2.pdf)

[10] Smith, H. J., Dinev, T., and Xu, H. (2011). Information privacy research: an interdisciplinary review. MIS Quarterly, 35(4), 989-1016.

[11] Saeri AK, Ogilvie C, La Macchia ST, Smith JR, Louis WR (2014). Predicting Facebook users' online privacy protection: risk, trust, norm focus theory, and the theory of planned behavior. J Soc Psychol. 154(4):352-69.

[12] Kusyanti, A., Haq. 2016. "How do I look": Self-disclosure of Instagram users in Indonesia. Journal of Education and Social Sciences, Vol. 5, issue 2, (October) ISSN 2289-1552

[13] Field, A., 2009. Discovering statistics using spss. 3rd ed. Sage Publications. (http://fac.ksu.edu.sa/sites/default/files/ktb_lktrwny_shml_fy_lhs.pdf)

[14] Oruç, Ö.E. and Tatar, Ç. 2017. An investigation of factors that affect internet banking usage based on structural equation modelling. Computers in Human Behavior, 66, p.232-235 (http://dx.doi.org.sci-hub.cc/10.1016/j.chb.2016.09.059)

[15] Kuo, Kuang-Ming. and Talley, P.C., 2014. An Empirical Investigation of The Privacy Concerns of Social Network Site Users in Taiwan. International Journal of Scientific Knowledge, 5(2) (http://ijsk.org/uploads/3/1/1/7/3117743/1_privacy_of_social_network_070414.pdf)

[16] Shin, D.H. The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. 2010. Vol. 22 No. 5, pp 428-438.

[17] Ayo, C.K., Mbarika, V.W. and Oni, A.A. 2015. The Influence of Trust and Risk on Intention to Use E-Democracy in Nigeria. Mediterranian Journal of Social Sciences, 6(6 S1), p.477 (http://www.mcser.org/journal/index.php/mjss/article/viewFile/8044/7709)