The Impact s of Requested Permission on Mobile App Adoption: The Insights Based on an Experiment in Taiwan

Hsiangchu Lai
National Taiwan Normal University
hclai@ntnu.edu.tw

Jack Shih-Chieh Hsu
National Sun Yat-sen University
Jackshsu@mis.nsysu.edu.tw

Min-Xun Wu
National Sun Yat-sen University
kusugawa1209@gmail.com

Abstract

Due to the popularity of smartphones, the number of apps has been growing up rapidly. Users have to grant requested permissions before downloading apps. However, some apps may request more permissions than they need. It may cause the concern of security or privacy. The purpose of this study is to investigate the impacts of requested permissions on users' intention to install mobile apps. We developed the proposed proposal by embedding the social exchange theory into technology acceptance model plus the concept of permission-function fit, perceived privacy-level and perceived privacy risk. We validated the proposed hypotheses with data collected from 389 smartphone users by using experimental design approach. The findings include (1) Users' attitude toward the app positively influences their download intention. (2) Users' perceived usefulness and the ranking of the app positively influence users' attitude toward the app while perceived privacy risk negatively affects users' attitude. Further, if the app requests more permissions than it needs, users have a negative attitude toward it. Overall, perceived usefulness has the strongest effect on attitude. (3) The privacy-level of the requested permissions positively affects users' perception of privacy risk. In addition, if there are over-requested permissions, users perceive higher privacy risk.

1. Introduction

Over the past years, due to the advances of network connections and popularity of smartphones, the number of apps has been growing up rapidly. Users can download different type of apps to accomplish different tasks. iOS and Android are the two leading operating systems of the smartphone market. Based on the statistics, the number of apps available in leading app stores as of March 2017, Android users were able to choose between 2.8 million apps while Apple's App Store has 2.2 million available apps [30]. In addition to built-in apps, there are many apps available to fulfill users' different purposes. According to Google Play's classification, apps are classified into 49 categories. The top five Google Play categories include education, lifestyle, entertainment, business and personalization [3]. When downloading or installing apps from either Apple's App Store or Google Play, users are always required to grant some permissions to install the app or perform specific functions because some apps may need to access operating system level functions of the mobile operating systems in order to provide services for users. For instance, a navigation app may have to get the functions related to either approximate or precise location to provide navigation service.

However, it is not rare that some apps request permissions have nothing to do with the provided functions. For instance, if a navigation app requests permissions related to sending SMS message, which is nothing with navigation, it is a kind of extra permission. We proposed a concept named "permission-function fit (PFF)" to describe the relationship between the functions provided by an app and the requested permissions. If the requested permissions fit the functions provided by the app, the PFF is "fit"; on the other hand, if an app requests more permissions than it really needs, the PFF is "over requested".

There are various kinds of permissions requested by apps. Some permissions are relevant to privacy, such as learning user's approximate location and reading text messages. In addition, the privacy-level of each permission is different. For instance, the privacy-level of permission to read text messages may be higher than that of permission to learn user's approximate location. Not all users feel comfortable to reveal personal information to apps that they do not understand well. In addition, users may have different concerns about the different privacy-levels of permissions. Information may be misused not only by the developers of those apps but also by the developers of other apps through an inter-app function-call approach [4].

As the apps are getting popular, it is important to learn how the apps' requests for permission impact the

URI: http://hdl.handle.net/10125/50378
ISBN: 978-0-9981331-1-9

users' adoption behavior. We want to understand whether users will give away their private information to exchange for better customized-services or keep away from the apps that request permissions relevant to privacy in order to protect their personal information. Therefore, the following are two purposes of this study: (1) To understand whether the privacy-level of requested permissions would influence users' intention to adopt apps. (2) To figure out what role PFF plays in users' intention to download apps.

2. Research model and hypotheses

Understanding the antecedents of downloading and keeping apps is one popular research stream recently [21]. For example individuals are more likely to adopt location-based application when their mobile self-efficacy is high [20]. Utility and habits block students to adopt mobile note-taking software [27]. Even personality has an impact on perceived benefits or perceived privacy, which then affects the intention to use a mobile app [25].

Apps can only access resources on the mobile phone after users grant permissions. Even though many users lean on not downloading an app that they are not familiar with, malicious developers may ask extra permissions by naming the app sounds like other famous apps, making the app looks like other famous apps, or even giving the app away for free [6]. Therefore, promoting users' awareness of permission became a salient issue.

Researchers spend significant efforts on understanding how to promote users' awareness of permission issue. For example, simply bringing privacy information can help mobile phone users to choose apps that request fewer permissions [19]. Users are more curious toward security-related information when they are presented with a risk-score toward the app [11]. However, those approaches focus on providing additional information to elicit users' awareness of risk issue. It is then valuable to explore whether users are aware of the permission issue without such additional information since, in general, the description of an app does not remind users the issues of privacy or risk that using this app may have.

Even studies based on Technology Acceptance Model (TAM) are too many and have been criticized for limited creative contributions, TAM could effectively explain users' intention to adopt information systems in different contexts [7] [12] [22] [28]. Therefore, we adopted TAM as the theoretical foundation of this research to understand the drivers of download intention. However, different from the original TAM, we did not include perceived ease of use but added perceived privacy risk into the model. For contemporary apps to be accepted by users, ease of use is one critical point. Since there are many similar apps in the app store, users can switch to another app easily. High competition drives developers to simplify the interface and make the app very easy to use. It is a must-be condition for competition and thus most apps are quite easy to use. Therefore, we believe that ease of use can be neglected in this condition. On the other hand, we included perceived privacy risk into the model because permission control directly associates with privacy issues, such as information leaking. Attitude is a summary of positive and negative beliefs. This implies that, in addition to benefits of adoption, users also take negative effects of adoption into consideration. The concern of privacy harms can be considered as one negative beliefs toward the app. Privacy concern has been shown to be one critical determinant of intention to download an app [13]. Furthermore, risk perception has been shown to have an impact on security-information awareness and app selection [11] [19]. Therefore, perceived risk is included in our research model.

In order to download or install apps, users have to grant permissions requested by apps. Granting permission is similar to the concept of exchange between cost and benefit mentioned in social exchange theory (SET) [5] [15]. According to SET, when individuals exchange resources with other people, they generally expect reciprocal benefits such as personal affection, trust, gratitude, or economic return [5] [18]. SET also stated that people would try to maximize their rewards and minimize their costs during the exchange [26]. It indicates that if PFF is fit, it is kind of fair exchange. If PFF is over-requested, users may feel that they pay more than what they will get, which may have a negative impact on their attitude toward the app.

Further, many requested permissions are related to privacy issues such as reading phone state and identity, modifying/deleting SD card contents, sending SMS Messages. Researchers indicated that privacy concern arises when consumers notice that their personal information is collected [1] [29]. Miyazaki and Fernandez also stated that network security and information privacy are the two major concerns for the consumers in an online shopping context [23]. Thus, if the requested permissions are related to privacy, users may develop concerns about information privacy and then increase perceive privacy risk of downloading it. In general, users may concern about higher perceived risk due to the unfair exchange, the over-requested permissions.

Either Apple's App Store or Google Play allows users to evaluate the quality of apps in the ranking

systems. These rankings help users to understand others users' perceptions and then decide whether to install apps or not. The rankings are similar to electronic Word-of-Mouth (eWOM). Researchers have indicated that WOM has an effect on consumers' attitude toward products and services [24]. It indicates that the ranking of apps may influence users' attitude toward downloading apps. As shown in Figure 1, a research model was proposed based on above discussions. Moreover, through the proposed research model, we also can understand how these constructs impact users' intention to download apps and the relative importance of these constructs.

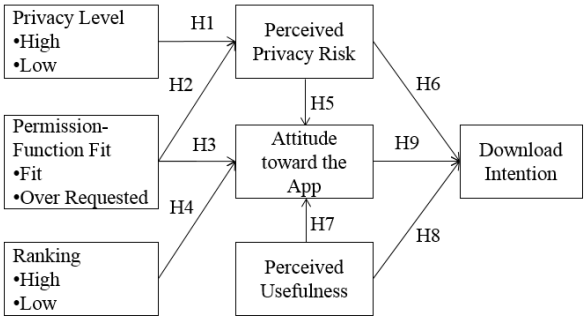

Figure 1. Research model

Based on above discussions, the following hypotheses were proposed:

H1: The privacy-level of permissions requested by an app positively influences users' perceived privacy risk of downloading it.

H2: An app with over requested PFF will let uses perceive higher privacy risk than the one with fit PFF.

H3: Users will have more positive attitude toward an app with fit PFF than the one with over requested PFF.

H4: The ranking of an app positively influences users' attitude toward it.

H5: Users' perceived privacy risk of using an app negatively influences their attitude toward it.

H6: Users' perceived privacy risk of using an app negatively influences their intention to download it.

H7: Users' perceived usefulness of an app positively influences their attitude toward it.

H8: Users' perceived usefulness of an app positively influences their intention to download it.

H9: Users' attitude toward an app positively influences their intention to download it.

3. Research methodology and data collection

3.1. Experimental design

We adopted an online experimental method to understand the effects of permission-function fit (PFF), privacy-level of permissions requested (PL) and app rankings on users' intention to download apps. In this online experiment, a scenario describing the need for downloading a bookkeeping app was provided first. Subjects were asked to evaluate the app through reading according information and permissions that requested by the app. They then were requested to provide their perceptions and intention toward downloading the app. Lastly, they were debriefed and thanked for participating in this experiment.

The online experimental method is considered appropriate since this approach allows us to access different respondents and allows respondents to participate the experiment in a setting similar to their daily life. The artificial app was called NeGoGo bookkeeping, created mainly based on the appearance and content of a popular bookkeeping app in Google Play. To avoid possible bias caused by familiarity (some subjects may know this real app and possess an attitude toward it already) An artificial app was provided, instead of a physical app. Figure 2 presents the functions provided by NeGoGo Bookkeeping while Figure 3 shows the requested permissions.

Figure 2. Description about NeGoGo Bookkeeping

Figure 3. Permissions requested by NeGoGo bookkeeping

In the experiment, we manipulated the levels of PLs, PFFs and rankings for subjects to see whether those factors influence subjects' intention to download the bookkeeping app. Each group has its own PL (low or high), PFF (fit or over requested) and ranking (low or high). Thus, this is a 2 (PL) ×2 (PFF) ×2 (ranking) factorial designs. Totally, there were eight groups in the experiment (Table 1). To exclude possible bias, all subjects were randomly assigned into eight groups. Regarding the way to determine what permissions to be included in our study, we first checked the top 20 most requested permissions of top 50 free apps in the country. We then conducted a survey to investigate how users perceive the privacy-level of the popular permissions, which guide the way to design low/high privacy-level. For the group of "fit" PFF, we picked some permissions needed by NeGoGo Bookkeeping. On the other hand, we added some extra permissions that are not relevant to bookkeeping functions for the group of "over-requested" PFF. For ranking, the rating score were manipulated as 2.5 and 4.5 to represent low and high ranking separately.

Several strategies were adopted to assure that respondents can immerse into the setting. First, we created a website to simulate the App downloading conditions. Both the appearance of the website and the app downloading process were exactly same as they were in Google Play. Second, we carefully select the experimental app for bookkeeping since bookkeeping is a daily work that people are familiar with it. The app design was based on a popular bookkeeping app in Google Play in order to reduce the gap between the experimental app and the real case. However, we gave its name as NeGoGo Bookkeeping to avoid biases caused by familiarity. Third, we conducted several pilot tests and adjusted the procedure accordingly to increase validity and avoid possible biases.

In addition to demographic information, we had to measure four constructs. Items for all constructs were adapted from related studies and modified slightly to fit into the context of this study (see the appendix). In addition, all of them were measured on a seven-point Likert scale, anchored from "1" (strongly disagree) to "7" (strongly agree). Here are the references for each construct:

1. Perceived privacy risk: The items of this construct were based on [2] and [31]. Finally, there are six items.
2. Perceived usefulness: The finalized six items of this construct were based on [9].
3. Attitude toward the app: The items of this construct were based on [32]. Totally, this construct has four items.
4. Download intention: The items of this construct were based on [28]. There are four items.

3.2. Data collection and sample profile

The data had been collected for five weeks in 2014 through Facebook and Taiwan's famous BBS - PTT (https://www.ptt.cc/index.html). PTT was selected because it is the most popular BBS platform and the users of this platform locate in all areas of Taiwan. In addition, most PPT users are relatively young, which are the main users of Smartphone and Apps in Taiwan. We designed an incentive mechanism to assure we can recruit a sufficient number of participants and increase participants' engagement in the whole experiment process. Respondents had the chance to receive various prizes through a random drawing, as long as they finished the experiment, completed the questionnaires, and correctly answered at least two manipulation items.

A total of 555 individuals participated in this study. As indicated above, a manipulation check with three items was used to verify whether respondents participated in the experiment carefully and with full attention. Subjects who did not correctly answer two or more manipulation check items were excluded. After dropping the invalid subjects, the sample has 389 valid respondents. Based on [14], to generate sufficient power, at least 16 cases for each condition (128 cases for 8 conditions) are needed for ANOVA and the total respondents should exceed 5 to 10 times of the number of indicators (200 cases for 20 items in this study) for structural equation modeling analysis. In this study, since the number of final valid respondents exceeds these requirements and therefore the result is sufficient

for the following statistical analyses. Table 1 contains the factorial design and number of respondent in each group.

Among the valid respondents, 51.4% are male, and 48.6% are female. Most of the participants are over 20 years old and have college or above degree. In addition to the default apps, almost all respondents downloaded more than six extra apps. Totally, 89.2% of respondents knew the concept of permissions in Android platform. However, only 55.0% of respondents considered the permissions when they downloaded apps. Table 2 shows the demographic information of our subjects.

Table 1. Factorial design and number of respondents in each group

Group	PLRP	PFF	Ranking	Number	Male	Female
1	Low	Fit	High	56	30	26
2	Low	Fit	Low	58	33	25
3	Low	Over Requested	High	53	29	23
4	Low	Over Requested	Low	53	22	31
5	High	Fit	High	42	20	22
6	High	Fit	Low	47	23	24
7	High	Over Requested	High	39	20	19
8	High	Over Requested	Low	41	23	18

PLRP: Privacy-level of Requested Permissions
PFF: Permission-Function Fit

Table 2. Demographic information

Measure	Categories	Number	%	Measure	Categories	Number	%
Gender	Male	200	51.4	No. of download apps	Under 5	20	5.1
	Female	189	48.6		6~10	106	27.2
Age	Under 20	80	20.6		11~15	99	25.4
	21~25	200	51.4		16~20	58	14.9
	26~30	71	18.3		Above 21	106	27.2
	31~35	29	7.5	Reason to download apps	Friends	47	12.1
	Above 35	9	2.4		App stores	318	81.7
Degree	High school	24	6.2		Online forum	19	4.9
	College	265	68.1		Others	5	1.3
	Graduate	80	20.6	Understanding the concept of permission	Yes	347	89.2
	Higher	20	5.1		No	42	10.8
				Considering the permission when downloading apps	Yes	214	55.0
					No	175	45.0

4. Data analysis and discussions

SPSS 22.0 and SmartPLS 2.0 were the tools to analyze data in this study. SmartPLS is used to analyze reliability, validity, and the relations among perceived privacy risk, perceived usefulness, attitude toward the app and download intention (H5-H9). SPSS was applied to analyzing the manipulated variables (privacy-level of requested permissions, permission-function fit, and ranking) in the experiment (H1-H4). Finally, SEM model was analyzed.

4.1. Measurement model

The adequacy of the measurement model was assessed by evaluating the reliability, convergent validity and discriminant validity [7]. Reliability testing was conducted on the data to examine the internal consistency between items expected to measure the same construct, and it was examined based on the composite reliability (CR) values which should be greater than 0.7. Table 3 shows that the CR values of all constructs are larger than 0.7. Therefore, the reliability of this study is assured.

Regarding convergent validity, the average variance explained (AVE) by each construct must

exceed 0.5 suggested by [10] and all indicator loadings would be significant and should exceed 0.7. In our research, there is evidence of convergent validity with the AVE for all factors exceeding 0.5, indicating that the majority of the variance was explained by the constructs. Additionally, our loading value of each item for its reflective construct was greater than 0.7.

Table 3. Descriptive statistics for constructs

Construct	Items	AVE	CR	Cronbach' α
Perceived Privacy Risk	6	0.769	0.952	0.940
Perceived Usefulness	6	0.679	0.927	0.905
Attitude toward the app	4	0.847	0.957	0.940
Download Intention	4	0.899	0.973	0.962

Regarding discriminant validity, we assessed it in two ways. First, the square root of the average variance extracted should be greater than all corresponding correlations. In our case, it was confirmed. The second way is to examine that the cross loading matrix has no item loaded more highly on another construct than it did on its associated construct. Based on these two tests, all constructs exhibited satisfied discriminant validity.

4.2. Structural model and hypotheses testing

SPSS and SmartPLS 2.0 were applied to measuring the coefficient and significant level of the proposed research model and testing hypotheses. The strength of paths coefficients between constructs was tested through SmartPLS. We examined the level of significance based on T-value. In addition, we also analyzed the impacts of independent variables by SPSS.

Relationships among Privacy Level (PL), Permission-function Fit (PFF) and Perceived Privacy Risk

ANOVA was used to assess whether different levels of PL, PFF, and ranking would lead to different levels of perceived privacy risk and attitude toward downloading the app. In ANOVA, whether the hypothesis is significant is determined through F-value and P-value. Table 4 shows that the relationship between PL and perceived privacy risk is F-value=36.518, and P-value < 0.001. It means different designs of PL differently influence perceived privacy risk. The mean of perceived privacy risk is 4.639 when PL is low. On the other hand, when PL is high, the mean of perceived privacy risk is 5.261. It means that when PL is low, users would perceive lower privacy risk. Thus, H1 is supported.

Similarly, the relationship between PFF and perceived privacy risk is F-value = 14.537, and P-value < 0.001 (Table 4). The mean of perceived privacy risk with over-requested PFF (5.107) is higher than the one with "fit" PFF (4.728). It also means that when PFF is over-requested, users would perceive higher privacy risk and thus H2 is supported too. However, the insignificant of the interaction term implies that PFF and PL do not affect perceived privacy risk jointly.

Table 4. ANOVA analysis of the effect of PL and PFF on perceived privacy risk

Source	Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	52.242[a]	3	17.414	16.813	.000
Intercept	9383.435	1	9383.435	9059.451	.000
PFF	15.057	1	15.057	14.537	**.000**
PL	37.824	1	37.824	36.518	**.000**
PFF * PL	.935	1	.935	.902	**.343**
Error	398.768	385	1.036		
Total	9827.097	389			
Corrected Total	451.010	388			

a. R Squared = .116 (Adjusted R Squared = .109)
PFF: permission-function fit
PL: privacy-level of requested permissions

Relationships among PFF, Ranking, and Attitude

Based on ANOVA analysis, Table 5 shows that the relationship between PFF and attitude is F-value=5.347, and P-value<0.05. The mean of attitude is 4.531 when PFF is over-requested. When PFF is fit, the mean of attitude turns out to be 5.003. It means users have a more positive attitude when PFF is fit. Therefore, H3 is supported. In addition, the relationship between ranking and attitude is F-value=17.636 and P-value=<0.001. The mean of attitude with a high ranking (5.026) is greater than the one with low ranking (4.539). Thus, there is a significant positive relationship between ranking and attitude. That is, users will have a more positive attitude when the ranking is high and thus H4 is supported. Finally, Figure 4 summarizes the path coefficients of the

proposed research model. It indicates that all hypotheses are supported (Table 6).

Table 5. ANOVA analysis of the effect of PFF and ranking on attitude

Source	Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	231.955[a]	4	57.989	89.111	.000
Intercept	30.860	1	30.860	47.423	.000
PFF	3.480	1	3.480	**5.347**	**.021**
Ranking	11.477	1	11.477	**17.636**	**.000**
PU	145.621	1	145.621	223.776	.000
PPR	27.668	1	27.668	42.517	.000
Error	249.887	384	.651		
Total	9358.688	389			
Corrected Total	481.842	388			

a. R Squared = .481 (Adjusted R Squared = .476)

PFF: permission-function fit, PU: perceived usefulness,
PPR: perceived privacy risk

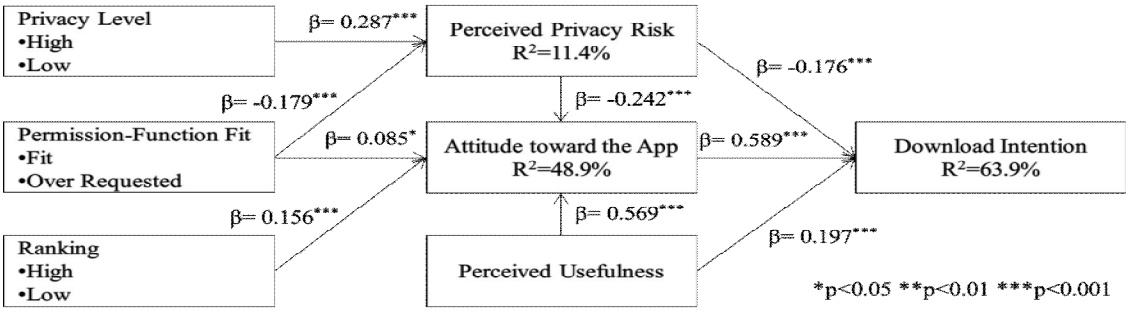

Figure 4. Structural model

Table 6. Results of hypotheses testing

	Hypotheses	Result
H1	The privacy-level of permissions requested by an app positively influences users' perception of privacy risk of downloading it.	supported
H2	Users will perceive higher privacy risk with an app with over requested PFF than one with fit PFF.	supported
H3	Users will have more positive attitude toward an app with fit PFF than one with over requested PFF.	supported
H4	The ranking of an app positively influences users' attitude toward it.	supported
H5	Users' perception of privacy risk of using an app negatively influences their attitude toward it.	supported
H6	Users' perception of privacy risk of using an app negatively influences their intention to download it.	supported
H7	Users' perception of usefulness of an app positively influences their attitude toward it.	supported
H8	Users' usefulness of an app positively influences their intention to download it.	supported
H9	Users' attitude toward an app positively influences their intention to download it.	supported

4.3. Discussions

There are three observations in the main findings of this study. First, users' intention to download an app is influenced by perceived privacy risk, perceived usefulness and users' attitude toward it. Among these

factors, user's attitude toward an app has the strongest effect while perceived privacy risk has the weakest effect. Second, users' attitude toward downloading an app is a function of perceived usefulness, ranking, PFF and perceived privacy risk. Among those four antecedents, perceived usefulness has the strongest effect and PFF has the weakest effect on attitude. Third, perceived privacy risk is determined by both of the privacy level (PL) of permissions requested by apps and PFF. Between these two relationships, PL has the stronger effect.

Permissions management is one research stream in mobile app studies. Previous studies have shown that showing privacy information help mobile phone users to choose apps that request fewer permissions [19]. Users are more curious toward security-related information when they are presented with a risk-score toward the app [11]. In this study, we moved further and proposed the importance of function-permission fit. We argued that users generate a sense toward the permissions needed by a specific app. Specifically, based on the functions that an app provides, users evaluate whether the permissions requested by the app is reasonable. The results confirmed our expectation that users tend to trust the app more and their attitude toward downloading the app is higher when permissions asked by the app fit with functions provided.

In addition to the fit between permissions and functions, we also showed that the type of permission that one app asks for is also critical. If an app asks for more sensitive permissions, users are more likely to find this app suspicious since their level of perceived risk is high. This again highlights the importance of presenting the contained functions on the description page, especially those functions related to the asked permissions.

Third, past studies in app adoption and continue usage highlighted the importance of having appropriate functions [17]. In this study, we further illustrated that the functions one app contains also reflect the permission that the app should ask for. As the experience with mobile app increases, users develop a sense of what permission that one app should ask for. Therefore, in the app description page, developers should clearly present their main functions and specify functions that require extra permissions. If they can clearly address that the permissions asked fit with the functions of the app, users tend to sense less privacy risk, and their attitude toward downloading the app is higher.

5. Conclusions

The purpose of this study is to investigate the impact of permissions on users' intention to download apps. All hypotheses in the proposed research model are supported. This study contributes to academia and practitioners in the following ways.

To researchers, there are four valuable implications generated from our findings. First, this study introduces a new concept named permission-function fit (PFF). The result indicates that PFF is the antecedent of perceived privacy risk. Moreover, although the effect of PFF is not as large as expected, PFF does have an effect on users' attitude toward an app, both directly and indirectly through privacy risk. The combination of these two effects are still considerable. We successfully demonstrated that users sense a higher level of risk when the requested permissions are significantly more than the functions provided. Such results align with the finding of previous studies. For example, showing privacy information or presenting risk-score allow users to be aware of the security issue [19]. Future research may extend the fit idea and study the fit between function and other features of an app. Second, users' attitude toward an app is positively influenced by perceived usefulness and ranking, but negatively influenced by perceived privacy risk. PFF-fit results in a more positive attitude than the over-requested one. Furthermore, attitude is primarily influen18ed by perceived usefulness. That is, when downloading apps, perceived usefulness is the major concern for users. This implies that TAM is still useful on predicting downloading intention. However, other critical antecedents should be incorporated into the model as well. Third, perceived privacy risk is negatively influenced by the privacy level of permissions requested by apps. If an app requests too many privacy-related permissions or the permissions are over-requested, users tend not to download the app because they perceive higher level of privacy risk.

To practitioners, there are two suggestions. First, users' download intention is determined by their attitude toward the apps. It means if the developers of apps want to increase users' download intention, they should manage to improve users' attitude toward the app. If developers want to improve users' attitude toward the app, they should improve users' perceived usefulness of the app, which means they have to consummate the information page of the app. Besides, they should increase the ranking of the app through better marketing and customer service. Second, perceived privacy risk is influenced by the privacy-level of permissions requested by apps and PFF. If an app requests too many privacy-sensitive permissions, it reduces users' willingness to use the app. Moreover, if the PFF of an app is over requested, users may

perceive more privacy risk. Thus, if an app needs some permissions relevant to privacy in order to work properly, the developers should explain why the app needs the permissions as clearly as they can in order to reduce users' perception of privacy risk. Lastly, our survey also shows that, even though most users are aware of permission issue, a number of users still ignore the permission information while installing new apps. Therefore, app store should pay attention to leading users to permission information, or even change the way to obtain users' permissions.

6. Appendix - Measurement

Perceived usefulness
1. The bookkeeping App enables me to accomplish bookkeeping task more quickly
2. The bookkeeping App improve my bookkeeping task performance
3. The bookkeeping App save my time on bookkeeping
4. The bookkeeping App is useful for bookkeeping
5. The bookkeeping App make bookkeeping easier
6. The bookkeeping App would enhance my bookkeeping effectiveness

Perceived privacy risk
1. I believe the bookkeeping App may give me personal information away without my permission
2. I believe the bookkeeping App may harm my privacy
3. Providing my personal information to the App may cause a lot of uncertainty
4. I may be involved in many problems after providing my personal information to the App
5. Providing my personal information to the App is risky
6. Providing my personal information to the App may cause a lot of potential losses

Attitude
1. I think this bookkeeping App is nice
2. I think this bookkeeping App is likable
3. I think this bookkeeping App can satisfy me
4. My attitude toward the App is positive

Intention
1. I will use the bookkeeping App if I have chance
2. I will use the bookkeeping App in the near future
3. I am willing to use the bookkeeping App in the near future
4. I will use the bookkeeping App when it is needed

Acknowledgements: This research was supported by the Ministry of Science and Technology under grant number NSC 103-2410-H-003-049-MY2.

7. References

[1] Agarwal, R., & Karahanna, E. Time Flies When You're Having Fun: Cognitive Absorption and Beliefs about Information Technology Usage. MIS Quarterly, 24(4), 2000, pp. 665-694.

[2] Aldás-Manzano, J., Lassala-Navarré, C., Ruiz-Mafé, C., & Sanz-Blas, S. The role of consumer innovativeness and perceived risk in online banking usage. International Journal of Bank Marketing, 27(1), 2009, pp. 53-75.

[3] AppBrain, Most popular Google Play categories, https://www.appbrain.com/stats/android-market-app-categories, 2017, Retrieved June 15, 2017.

[4] Bagheri, H., Sadeghi, A., Garcia, J., & Malek, S. CONVERT: Compositional Analysis of Android Inter-App Permission Leakage. IEEE Transactions on Software Engineering, 41(9), 2015, pp. 866-886.

[5] Blau, P. M. Exchange and power in social life: Transaction Publishers, 1964.

[6] Chia, P. H., Yamamoto, Y., & Asokan, N. Is this app safe?: a large scale study on application permissions and risk signals. In Proceedings of the 21st international conference on World Wide Web, ACM, April, 2012, pp. 311-320.

[7] Chiu, C. M., Chang, C. C., Cheng, H. L., & Fang, Y. H. Determinants of customer repurchase intention in online shopping. Online Information Review, 33(4), 2009, pp. 761-784.

[8] Chiu, C.-M., Lin, H.-Y., Sun, S.-Y., & Hsu, M.-H. Understanding customers' loyalty intentions towards online shopping: an integration of technology acceptance model and fairness theory. Behaviour & Information Technology, 28(4), 2009, pp. 347-360.

[9] Davis, F. D. Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Quarterly, 13(3), 1989, pp. 319-340.

[10] Fornell, C., & Larcker, D. F. Evaluating structural equation models with unobservable variables and measurement error. Journal of Marketing Research, 18(1), 1981, pp. 39-50.

[11] Gates, C. S., Chen, J., Li, N., & Proctor, R. W. Effective risk communication for android apps. IEEE Transactions on dependable and secure computing, 11(3), 2014, pp. 252-265.

[12] Gefen, D., Karahanna, E., & Straub, D. W. Trust and TAM in online shopping: an integrated model. MIS Quarterly, 27(1), 2003, pp. 51-90.

[13] Gu, J., Xu, Y., Xu, H., Zhang, C., & Ling, H. Privacy Concerns for Mobile App Download: An Elaboration Likelihood Model Perspective, Decision Support Systems, (94), 2017, pp. 19-28.

[14] Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. Multivariate Data Analysis, Pearson Prentice Hall, 2009.

[15] Homans, G. C. Social Behavior as Exchange. American journal of sociology, 63(6), 1958, pp. 597-606.

[16] Hsiao, C. H., Chang, J. J., & Tang, K. Y. Exploring the influential factors in continuance usage of mobile social Apps: Satisfaction, habit, and customer value perspectives. Telematics and Informatics, 33(2), 2016, pp. 342-355.

[17] Hsu, J., Lin, T. C., Fu, T. W., & Hung, Y. W. The effect of unexpected features on app users' continuance intention. Electronic Commerce Research and Applications. 14(6), 2015, pp. 418-430.

[18] Hsu, C.-L., & Lu, H.-P. Why do people play on-line games? An extended TAM with social influences and flow experience. Information & Management, 41(7), 2004, pp. 853-868.

[19] Kelley, P. G., Cranor, L. F., & Sadeh, N. Privacy as part of the app decision-making process. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM, 2013, pp. 3393-3402.

[20] Keith, M. J., Babb, J. S., Furner, C.P., & Abdullat, A. The role of mobile self-efficacy in the adoption of location-based applications: an iPhone experiment. In Proceedings of the 44th Hawaii International Conference on System Sciences, 2011, pp. 1-10.

[21] Kim, S. C., Yoon, D., & Han, E. K. Antecedents of mobile app usage among smartphone users. Journal of marketing communications, 22(6), 2016, pp. 653-670.

[22] López-Nicolás, C., Molina-Castillo, F. J., & Bouwman, H. An assessment of advanced mobile services acceptance: Contributions from TAM and diffusion theory models. Information & Management, 45(6), 2008, pp. 359-364.

[23] Miyazaki, A. D., & Fernandez, A. Consumer Perceptions of Privacy and Security Risks for Online Shopping. Journal of Consumer Affairs, 35(1), 2001, pp. 27-44.

[24] Nepomuceno, M. V., Laroche, M., & Richard, M.-O. How to reduce perceived risk when buying online: The interactions between intangibility, product knowledge, brand familiarity, privacy and security concerns. Journal of Retailing and Consumer Services, 21(4), 2014, pp. 619-629.

[25] Pentina, I., Zhang, L., Bata, H., & Chen, Y. Exploring Privacy Paradox in Information-sensitive Mobile App Adoption: A Cross-cultural Comparison, Computers in Human Behavior, 65, 2016, pp. 409-419.

[26] Salam, A., Rao, R., & Pegels, C. An investigation of consumer-perceived risk on electronic commerce transactions: The role of institutional trust and economic incentive in a social exchange framework. AMCIS 1998 Proceedings, 1998, p. 114.

[27] Schepman, A., Rodway, P., Beattie, C., & Lambert, J. An Observational Study of Undergraduate Student's Adoption of (mobile) Note-taking Software, Computer in Human Behavior, 28(2), 2012, pp. 308-317.

[28] Schierz, P. G., Schilke, O., & Wirtz, B. W. Understanding consumer acceptance of mobile payment services: An empirical analysis. Electronic Commerce Research and Applications, 9(3), 2010, pp. 209-216.

[29] Smith, H. J., & Milberg, S. J. Information privacy: measuring individuals' concerns about organizational practices. MIS Q., 20(2), 1996, pp. 167-196.

[30] Statista, Number of apps available in leading app stores as of March 2017, https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/, Retrieved June 15, 2017.

[31] Xu, H., Teo, H.-H., & Tan, B. Predicting the Adoption of Location-Based Services: The Role of Trust and Perceived Privacy Risk. ICIS 2005 Proceedings, 2015, pp. 897-910.

[32] Yang, B., Kim, Y., & Yoo, C. The integrated mobile advertising model: The effects of technology- and emotion-based evaluations. Journal of Business Research, 66(9), 2013, pp. 1345-1352.