

# The Effect of Privacy Concerns on Smartphone App Purchase in Malaysia: Extending the Theory of Planned Behavior

<https://doi.org/10.3991/ijim.v11i5.6961>

Zakariya Belkhamza <sup>(✉)</sup>, Mohd. Adzwin Faris Niasin  
Universiti Malaysia Sabah, Kota Kinabalu, Malaysia  
zakariya@ums.edu.my

**Abstract**—The rise of m-commerce has brought the intention to the issue of privacy concerns among mobile users, and studies showed that it is an important factor that affects attitude and intention to purchase smartphone apps. The objective of this paper is to investigate the issue of privacy concerns on the attitude and purchasing intention among Malaysian smartphone users. This paper employed the Theory of Planned Behavior (TPB) to investigate the role of privacy concerns in influencing the decision making process. The paper provides significant insights on the issue of privacy concerns in the usage of smartphones which can help developers such as Google and Apple to improve their apps stores to provide better protection for users' privacy and security in Malaysia.

**Keywords**—privacy concerns, purchase intention, theory of planned behavior

## 1 Introduction

As more consumers embrace the rise of the Internet era, the online privacy concerns remains a top priority for every smartphone user [1]. Many companies find it difficult to ensure privacy and security on their apps for their users to use and engage in a successful transaction, especially where cybercrimes are fast increasing. Privacy concerns naturally become an important issue as e-commerce makes it ascent into an important business aspect of most organizations. This is due to the fact that marketers are collecting more information on customers who are buying online to study not only their characteristics, but also their purchase preferences and behaviors. These concerns have proven to have negative consequences for the adoption of e-commerce [2], [3]. In Malaysia alone, it was reported by Malaysian Communication and Multimedia Communication agency (MCMC) that the country has a 35% of smartphone penetration, resulting to more than 10 million smartphone users. It is even predicted that smartphone penetration in Malaysia will rise to 60% by 2015. The statistics also reveals that Malaysia holds a 66% of Internet users from the population, with 60% internet penetration and 140% mobile penetration, with 47% of Malaysians own more than one mobile phone [4], [5]. Of the current smartphone users, 50.9% of them have

installed 10 to 30 apps in their smartphones [4]. In another investigation, the Wall Street Journal examined 101 popular smartphone apps and found out that 56 apps transmitted the phone's unique identifiers to other companies without users' awareness, while about 47 apps transmitted the device's location to outsiders [6], [7]. Furthermore, the study revealed that both Apple iOS and Google Android mobile operating systems regularly record and transmit location data without the consent of phone owners. These findings represent concerns regarding users' information privacy, especially when MCMC stated that most Malaysian smartphone users tend to opt for "jailbreak" smartphones that allow the downloading of apps which have not been approved by app stores as these apps may impose security and data integrity risks [4]. This confirms that the increasing number of smartphone users will only lead to the increasing of privacy risks [8], [9].

In addition to these alarming statistics, the lack of academic research on the influence of privacy concerns on consumers' intention to purchase smartphone apps still suffer from a holistic understanding of the issue, especially when including other influential factors that affect the decision to purchase apps such as the stimulus of social influences and one's own perceived ability to perform the behavior. Although there are significant number of theories and research on the effect of privacy concerns on purchase intention in the general concept of information systems and e-commerce [10], there is a little evidence if the findings of those studies still hold true in the mobile technology context [11]. Known past studies lack the attempt and initiative to investigate and examine the role of privacy concerns on smartphone apps purchase intention by integrating a theoretical predictive consumer behavior framework such as the Theory of Planned Behavior (TPB) in the context of smartphone privacy. Despite the existence of several studies that used TPB on mobile devices related topics, they do not explicitly studied the effect of privacy concerns on smartphone apps purchase intention [12], [13].

On this regard, the objective of this paper is twofold. The first is to investigate the issue of privacy concerns on the purchase intention of smartphone apps. More precisely, the aim is to give further insights on the issue of privacy concerns in the usage of smartphone apps stores which can help developers such as Google and Apple to improve their apps stores to provide better protection for users' privacy and security in Malaysia. The second objective of the paper is to provide a better understanding on the role of privacy concerns and perception towards the purchase or usage behavior among Malaysian smartphone users through the utilization of the Theory of Planned Behavior as the roles of perceived behavioral control and subjective norm are also taken into consideration.

## **2 Literature review**

### **2.1 The concept of privacy concerns**

Privacy has long been identified as a moral right [14]. As far as technology is concerned, ref [15] defined it as "the moral right of individuals to be left alone, free from

surveillance or interference from other individuals or organizations, including the state". Specifically, it is the concerns of users on the collection, usage and manipulation of personal information by firms or entities due to the fear of loss or threat or breach of privacy. This definition is tailored toward its information aspects, rather than its physical, legal, and behavioral aspects [16]. Ref [17] identified four core measurements for dimension of individual privacy or "concerns for information privacy" (CFIP) where these dimensions have been widely used by researchers in general [18]. These measurements are collection, improper access, errors and secondary use. Collection in the context of information privacy can be defined as the concerns related to the huge amount of personal information collected and stored in the company's database. Similarly, improper access is the concern that the collected information becomes accessible to unauthorized people. Errors concerns the perception that personal information related to individuals may become incorrect due to unintentional or malicious alterations. Finally, secondary use is the concern on the way the collected personal information is used by a third party for other purposes other than the initial intention [17]. The context of this relationship in information privacy has also gained attention in the literature. Ref [17] validated the construct of the use of behavioral intentions to measure individuals' tendencies to be skeptical in dealing with technology, which could be used to gather, share their personal information. This construct, which was mainly derived from [19] is being widely used in the literature to explain the user behaviors with technologies across various contexts [20], [21], [22].

On this regards, considerable attention has been paid to the issue of privacy concerns and security on smartphones [9], [23]. It was found that many users who have downloaded apps from app stores such as Google Play and Apple's App Store have low concerns on privacy. This is because they tend to disregard security alerts when they install apps from these app stores, with most of them unable to understand the risks and privacy issues associated with that installation [24], [23]. These studies suggested that users are more concerned about their privacy on their computers compared to their smartphones. It was further concluded that users believed that smartphones and personal computers are different. What makes smartphone users different is that they are exposed by considerable vulnerabilities and exposures through the traditional hacking, malwares and spywares, while at the same time are vulnerable to collection and dissemination of personal information by smartphone apps [25]. Google for instance has reportedly provided Australian developers with customer's personal information which included e-mail addresses [26]. On the other hand, iPhone users are exposed to privacy breach threats as the smartphone's Unique Device Identifier (UDID) of the device can reveal user's behavioral patterns and information if exploited based on apps usage or the device itself [27]. According to a recent study conducted by Pew Internet Project [28], more than half of smartphone users decided to uninstall apps from their smartphones due to the concerns of personal information with 54% deciding to forego apps installation while 30% of users uninstall apps when privacy became a concern. Another report by Hewlett-Packard found out that 9 out of 10 smartphone apps are vulnerable to privacy issues [28].

## 2.2 Theory of planned behavior

The Theory of Planned Behavior (TPB) [29] was developed with the goal of predicting the intentions and behaviors of individuals over a multitude of scenarios in a real life environment. TPB is extended from the original Theory of Reason Action (TRA) [30], [31] due to TRA's limitations and lack of effectiveness in handling individuals' behaviors where they are having incomplete control over those behaviors [32], [33]. It is widely acknowledged that TPB has been used by many researchers in its consistency to predict the intentions and individuals in a variety of situations [33], [34]. According to TPB, an individual's behavior to perform an action is determined by the individual's intention to accomplish the behavior whereas the intention is based on the attitude, subjective norm and the perceived behavioral control of the individual [29]. Attitude refers to the positive or negative connotation or feeling that an individual possess in performing a behavior [29], [35]. Subjective norm is the normative belief of an individual that is influenced by other people and social pressure to perform a given behavior; it can reflect the desire of oneself to perform certain actions which are dependent on whether people perceive the actions as favorable or not [29], [34]. On the other hand, perceived behavioral control is defined as an individual's perception of his or her own capability to perform a behavior of interest [29]. It includes the perception of resources, knowledge and facilitating conditions required to perform the behavior [13]. Research on the behavioral intention and attitude is well established in the literature [29], [30]. This establishment also includes information systems and technology adoption [35], [36]. These studies in the IT adoption context further confirm the old notion that the relationship between attitudes and intentions is based on the human need to achieve cognitive consistency [37].

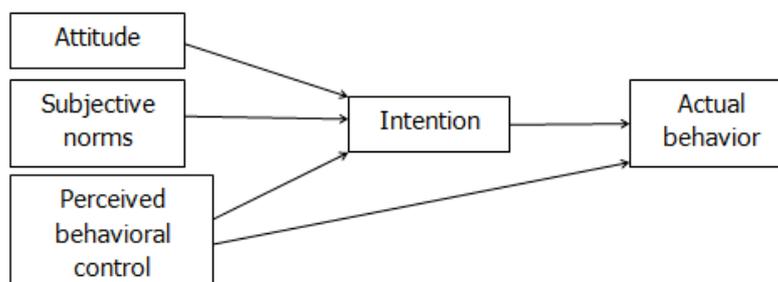


Fig. 1. Theory of planned behavior

## 3 Theoretical framework and conceptual development

The literature reports inconsistency of findings on whether privacy concerns has a relationship with the behavioral intention. [38] for instance reported that a majority of the privacy concerns dimensions were found to have no relationship with consumers' intention to perform online purchasing act. Yet, [39] found a negative relationship between privacy concern and intention to transact in an online environment. Con-

sistent with prior research [21] and [40], individuals who are concerned about their personal information privacy would refrain from keeping their personal identifiable information from their online transactions in order to protect their identity. Thus, it is hypothesized that:

*H<sub>1</sub>: There is a significant relationship between privacy concerns dimensions and smartphone apps purchase intention.*

The effect of privacy concerns on attitude or intention had been discussed in the literature and has resulted to some interesting findings (e.g. [41] and [33]). [42] found that the attitude of consumers towards direct marketing is negatively associated with the degree of concerns on privacy. This negative influence of privacy concerns over attitude was also confirmed by [41] when they investigated consumers' attitude towards websites for e-mail campaigns. Similarly, [43] have argued that individuals with stronger concerns about information privacy tend to exhibit negative attitudes about using a technology. Therefore, it is hypothesized that:

*H<sub>2</sub>: There is a significant relationship between privacy concerns dimensions and attitude towards smartphone apps purchase.*

Some studies did find that subjective norm does have an influence on the intention to implement technology-related behaviors [34], [13]. [13] has stated that referent power of peers' suggestions and recommendation will have a significant effect on manipulating an individual's decision to adopt new technology or services. In the context of mobile related issues, this appears to hold true in the context of this study since social norms was found to have a positive impact on the intention to adopt mobile shopping habit. Therefore, it is hypothesized that:

*H<sub>3</sub>: There is a significant relationship between subjective norm and smartphone apps purchase intention.*

There have been several studies confirming that that perceived behavioral control has an influence on the individual's intention to perform certain behaviors, specifically in the context of information technology-related topics [33], [34], [13], [44]. Ref [34] indicated that perceived behavioral control on buying product from a Web merchant positively influences the intention to buy products from the Web merchant. In addition, ref [13] confirmed that perceived behavioral control has a direct positive influence on an individual's intention to perform mobile shopping. Therefore, it is hypothesized that:

*H<sub>4</sub>: There is a significant relationship between perceived behavioral control and smartphone apps purchase intention.*

In the context of online shopping or e-commerce, several literatures have provided the basis that attitude affects intention to perform behavior. For example, [33] has indicated that when users have positive attitude towards online shopping, the intention of the users to shop online will increase, provided that the users' trustworthiness towards the privacy concern on online shopping is high. Additionally, other researches

on information technology-based behaviors have supported the notion that attitude has a positive effect towards intention [45], [33], [34], [13]. Therefore, it is hypothesized that:

*H<sub>5</sub>: There is a significant relationship between attitude and smartphone apps purchase intention.*

Attitude has been proven to exhibit the capability to mediate the relationship between two variables in multiple contexts such as online learning and online shopping. Ref [46] revealed that attitude mediates the relationship between the likelihood to abort online transaction and other predictors (i.e. information control and effort saving). Therefore, it is hypothesized that:

*H<sub>6</sub>: Attitude towards smartphone apps purchase mediates the relationship between privacy concern dimensions and smartphone apps purchase intention.*

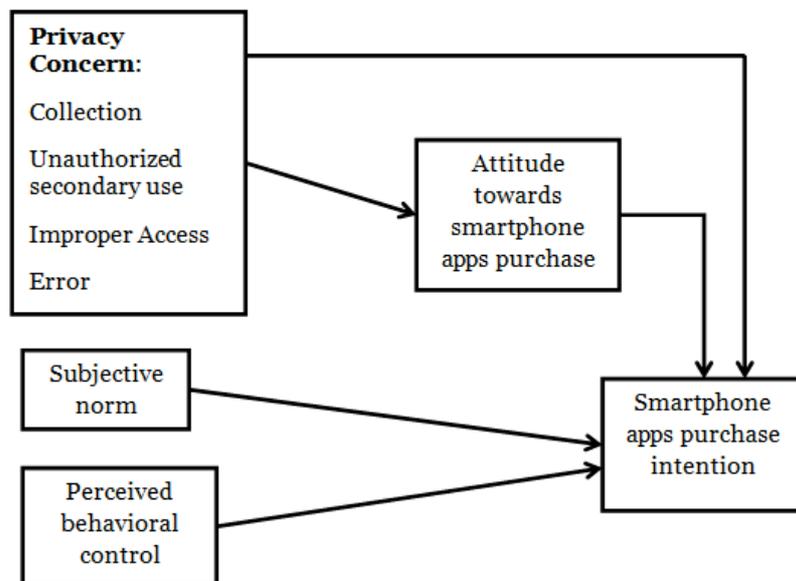


Fig. 2. Research framework

## 4 Methodology

The respondents targeted for this research are consumers who have experienced purchasing and installing smartphone apps through apps stores or repositories such as Google Play Store and Apple Store. Thus, the unit of analysis for this research is individual consumers aged between 20 to 40 years old since these consumers have the capability to acquire not just free apps but also paid apps. These individuals also have a better experience in using smartphones. The study used survey instrument to test the research hypotheses in accordance to the practice in the information privacy literature

[17]. Measurement scales were adapted from prior research. This has been made to ensure the measurements are valid and reliable. Items measuring attitude towards app purchase were adopted from [46]. The measurement items for app store purchase intention were adopted from [13]. Finally, measurement items for information privacy concerns were adapted from [17]. All items were measured using a five-point Likert scale from “Strongly disagree” = 1 to “Strongly agree” = 5. The questionnaire was distributed to a pool of Malaysian customers in three different geographical locations in Malaysia, namely, the capital Kuala Lumpur, the state of Selangor and the state of Sabah. Both non-probability convenience sampling and snowball sampling were used to collect data because both have been widely used in investigating consumer behaviors on e-commerce related issues [45], [33]. Furthermore, those types of sampling techniques were necessary to ensure the customer must fulfill the research criteria.

## **5 Results**

### **5.1 Profile of Respondents**

Out of 1200 questionnaire sets sent, 457 respondents were received. After dropping 7 for incompleteness, 450 usable respondents were used for the data analysis. The analysis of the respondents' demographics reveals that 54.7% of the respondents are male, while 45.3% are female. This indicates an adequate balance of the two genders. Most respondents are aged between 21 and 29 years old (58.0%); 36% of respondents have undergraduate degree followed by diploma holders at 30.7%; more than half of the respondents (56.7%) have steady monthly income (i.e. public / private / self-employed).

### **5.2 Smartphone Apps Usage**

This section provides statistical information on the smartphone usage of respondents who have participated in the study. The results indicate that the highest percentage of chosen app store is Google Play Store with 71.3% followed by the Apple Store with 20.0%. Google Play Store indicates that respondents use Android-based smartphones whereas Apple Store represents Apple's iPhone-based smartphones. The higher usage of Android-based smartphones among Malaysian is consistent with the reports of MCMC of the Malaysia 2013 headphones survey where the majority of Malaysian use Android-based phone at 79.2%. The other 8.7% consists of BlackBerry World (Symbian-based), Window Stores (Windows Phone-based), among others.

### **5.3 Reliability analysis**

The values for all constructs and their variables are presented in Table 1. It can be seen that all values are above the recommended value of 0.8, which shows a good reliability consistency [47].

**Table 1.** Reliability analysis

Construct	Variables	Number of items	Cronbach alpha
Privacy concerns	Secondary use	4	0.93
	Errors	4	0.88
	Unauthorized access	3	0.85
	Collection	4	0.82
Attitude	Attitude towards smartphone apps purchase	6	0.93
Subjective norm	Subjective norm	3	0.85
Perceived behavioral control	Perceived behavioral control	3	0.81
Intention	Smartphone apps purchase intention	3	0.87

#### 5.4 Descriptive analysis

The purpose of the descriptive analysis is to measure the mean and standard deviation for all the variables of the study. Based on the scale, mean that score lower than 2 indicate low responses, mean scores from 2 to 4 show moderate responses while mean scores higher than 4 represent high responses. The results compiled in Table 2 reveals that three variables have moderate mean scores ranging from the lowest to the highest respectively: smartphone apps purchase intention (2.99), attitude towards smartphone apps purchase (3.15) and errors (3.84). The rest of the variable showed high responses based on the mean scores that are higher than 4 which are collection (4.11), unauthorized access (4.40) and secondary use (4.47).

**Table 2.** Descriptive statistics

Variables	Mean	Standard deviation
Collection	4.11	0.70
Improper access	4.40	0.59
Unauthorized secondary use	4.47	0.58
Errors	3.84	0.87
Subjective norms	2.75	0.97
Perceived behavioral control	3.80	0.80
Attitude towards smartphone apps purchase	3.15	0.97
Smartphone apps purchase intention	2.99	0.93

#### 5.5 Multiple regression analysis

Multiple regression analysis was used to identify the relationship between the variables of the research model. The first hypothesis ( $H_1$ ) attempts to examine whether there is a significant relationship between privacy concerns dimensions and smartphone apps purchase intention. The results in Table 3 indicates that 6.0% of variances in smartphone apps purchase intention can be explained by privacy concerns ( $R^2 = 0.06$ ,  $p < 0.01$ ). Only the errors dimension of privacy concern is shown to be significant at  $p < 0.05$ , thus,  $H_1$  is partially supported.

**Table 3.** Multiple Regression Analysis for Hypothesis H<sub>1</sub>

Dependent variable	Independent variable	Std. Coefficient Beta ( $\beta$ )	t-value
Smartphone apps purchase intention	<b>Privacy concern:</b>		
	Collection	0.067	0.721
	Improper access	-0.078	-0.717
	Unauthorized secondary use	-0.054	-0.477
	Errors	0.244*	2.710
	$R^2$	0.06	
	Adjusted $R^2$	0.02	
	Significant F	0.11	

The second hypothesis (H<sub>2</sub>) attempts to examine whether there is a significant relationship between privacy concerns dimensions and the attitude towards smartphone apps purchase. The result in Table 5 indicates that 5.0% of variances in attitude towards smartphone apps purchase can be explained by privacy concerns ( $R^2 = 0.05$ ,  $p < 0.01$ ). Out of the four dimensions of privacy concerns, only unauthorized access dimension is found to have a negative influence on the attitude of respondents ( $\beta = -0.252$ ,  $p < 0.05$ ). The unauthorized access dimension has the largest unique contribution to explaining attitudes towards smartphone apps purchase as the part correlation value of -0.186 of the dimension suggests that the dimension contributed to 3.4% of variance in attitude. Therefore, H<sub>2</sub> is partially supported.

**Table 4.** Multiple Regression Analysis for Hypothesis H<sub>2</sub>

Dependent variable	Independent variable	Std. Coefficient Beta ( $\beta$ )	t-value
Attitude towards smartphone apps purchase	<b>Privacy concern:</b>		
	Collection	0.11	1.173
	Improper access	-0.252*	-2.301
	Unauthorized secondary use	0.187	1.658
	Errors	0.06	0.662
	$R^2$	0.05	
	Adjusted $R^2$	0.02	
	Significant F	0.11	

The hypothesis H<sub>3</sub> attempts to examine whether there is a relationship between subjective norms and smartphone apps purchase intention. The result in Table 5 indicates that 20.0 percent of variances in smartphone apps purchase intention can be explained by attitude where the subjective norms variable is shown to have significant relationship with purchase intention ( $R^2 = 0.20$ ,  $p < 0.01$ ). Therefore, H<sub>3</sub> is supported.

**Table 5.** Multiple Regression Analysis for Hypothesis H<sub>3</sub>

Dependent variable	Independent variable	Std. Coefficient Beta ( $\beta$ )	t-value
Smartphone apps purchase intention	Subjective norms	0.443**	6.007
	$R^2$	0.20	
	Adjusted $R^2$	0.19	
	Significant F	0.00	

The hypothesis H<sub>4</sub> attempts to examine whether there is a relationship between perceived behavioral control and smartphone apps purchase intention. The result in Table 4.15 indicates that 13.0 percent of variances in smartphone apps purchase intention can be explained by attitude where the subjective norms variable is shown to have significant relationship with purchase intention. ( $R^2 = 0.13, p < 0.01$ ). Therefore, H<sub>4</sub> is supported.

**Table 6.** Multiple Regression Analysis for Hypothesis H<sub>4</sub>

Dependent variable	Independent variable	Std. Coefficient Beta ( $\beta$ )	t-value
Smartphone apps purchase intention	Perceived behavioral control	0.357**	4.649
	$R^2$	0.13	
	Adjusted $R^2$	0.12	
	Significant F	0.00	

The hypothesis H<sub>5</sub> attempts to examine whether there is a relationship between attitude towards smartphone apps purchase and purchase intention. The result in Table 7 indicates that 36.0 percent of variances in smartphone apps purchase intention can be explained by attitude where the attitude variable is shown to have significant relationship with purchase intention with  $\beta$  value of 0.59 ( $R^2 = 0.36, p < 0.01$ ). Therefore, H<sub>5</sub> is supported.

**Table 7.** Multiple Regression Analysis for Hypothesis H<sub>5</sub>

Dependent variable	Independent variable	Std. Coefficient Beta ( $\beta$ )	t-value
Smartphone apps purchase intention	Attitude towards smartphone apps purchase	0.598**	9.068
	$R^2$	0.36	
	Adjusted $R^2$	0.35	
	Significant F	0.00	

### 5.6 Mediation analysis

In order to test the mediating role of attitude on the relationship between privacy concerns dimensions and smartphone apps purchase intention, a mediation analysis suggested by [48] is employed. The proposed method attempts to look at the values of Lower Level Confidence Interval (LLCI) and Upper Level Confidence Interval (ULCI) to establish a mediation effect of a variable. If there is no zero value between the two values, a mediation effect is established. This relationship suggests that attitude towards smartphone purchase mediate the relationship between the dimensions of privacy (collection, unauthorized access, secondary use and errors) and the intention to purchase apps. Table 8 summarizes the values of LLCI and ULCI for all four dimensions of privacy where the role of the mediating variable is designated for attitude. It can be seen that only the unauthorized access dimension of privacy concerns that does not have a zero value between the value of both LLCI (-0.444) and ULCI (-0.406). This indicates that attitude does have a mediation effect. For the other dimen-

sions, the zero values exist between the two values, which indicate that there is no mediation effect of attitude. Thus, Hypothesis H<sub>6</sub> is partially supported.

**Table 8.** Mediation Analysis for Hypothesis H<sub>6</sub>

Items	Effect	Standard Error	z-value	LLCI	ULCI
Collection	0.087	0.075	1.16	-0.367	0.254
Unauthorized access	-0.239	0.103	-2.321	-0.444	-0.406
Secondary use	0.181	0.110	1.645	-0.371	0.413
Errors	0.039	0.062	0.629	-0.088	0.156

## 6 Discussion

One of the main objectives of this paper was to examine and identify the smartphone apps purchase intention among smartphone users in Malaysia. It is important to note that this paper investigated both the relationship between privacy concerns and attitude towards app purchase and the relationship between privacy concern elements and apps purchase intention, which is one of the significance of this research. While numerous studies investigated app purchase intention instead of attitude, several of these studies found that attitude toward technology and intention to use IT are positively related [49].

The relationship between privacy concerns and attitude towards smartphone app purchase reported in this study was consistent with previous findings. The concerns for information privacy (CFIP) instrument [17], [21] were found to have a significant manifestation of privacy concerns in the mobile context. However, in this study, only unauthorized access was not found to have an influence on attitude. Similarly, the privacy concern’s significant relationship with purchase intention was only accounted for one dimension of the concerns for information privacy (CFIP), which is errors, while the others were found to be not significant. This is consistent with previous research which used The CFIP dimensions to mediate the relationship between computer anxiety and behavioral intentions [50].

These findings were not expected when looking at the trend of previous research [21], [51]. However, these findings need to be taken with caution for two reasons: The first reason is because attitude is modified as individuals obtain and process information regarding attitude objects [52]. This suggests that information privacy should be examined within different contexts to fully understand attitudes of individuals towards any business practice [53], [21]. Attitude in this sense is too delicate to catch the actual behavior of information privacy, especially when the technology is not well formed as the case for app purchase. To rectify this, ref [54] suggested expanding attitude to incorporate the concept of persuasion and ability, a sequence of changes occur in attitude. The second reason for looking at the results with caution is the nature of the information privacy dimensions themselves. The CFIP components are developed to capture the information privacy as reflective construct that may be more accurately modeled as a second-order factor rather than first-order dimensions [55], [21]. Moreover, the question of whether a directional change in one construct of the

whole dimension may imply similar directional shift in other constructs is applied in this dimensions [56].

Nevertheless, such findings on attitude are consistent with some previous research. Ref [57] found no significant relationship between users' concern for information privacy and their attitude towards using firewall protection for their electronic devices such as computers, although attitude was found to mediate the impact of perceived usefulness on behavioral intention. The findings of this study also confirm previous conclusions that individuals are concerned about information privacy as a general case and at an aggregate level, while the way in which individuals are concerned about collection, unauthorized secondary use, improper access, and errors require expanded consideration at the micro level of each dimensions [58]. This argument was also observed and justified by [59] where they observed the influence of cultural values of 38 countries including Malaysia in only errors and unauthorized secondary use, rather than the whole dimensions of the concerns for information privacy (CFIP). Similarly, [60] confirmed the significant differences between the concerns for information privacy (CFIP) in New Zealand and previous research of [21]. The current status of CFIP dimension may also justify the findings of this research to a great extent. Although the CFIP measurement was validated [21], [61], [20], the acknowledgement of [17] that the dimensionality of the scale has yet to be proven to be absolute still hold true. Nevertheless, this research significantly contributes to the proposal of [21] that the theoretical and operational assumptions of the concerns for information privacy should be reinvestigated in light of new technology and practice. The purchase behavior using apps is considered an emerging technology where such investigation may provide a better understanding on the dimension [62].

This paper was also able to demonstrate the ability of TPB to predict user's behavior to purchase smartphones apps. The result of the analysis has shown that the original constructs of attitude, subjective norm and perceived behavioral control in TPB were able of fully explaining the intention of smartphone users to purchase smartphone apps. It is proven that there is a significant relationship between attitude and intention to purchase smartphone apps. This finding is consistent with majority of the studies in the consumer-related behavior field as positive attitude is a usual indication for positive-oriented behavioral intention [29], [34], [63]. In terms of subjective norm, this study backs the finding by [64] where the authors revealed that the recommendation by other people generally influence the decision of users to download smartphone apps compared to other influences such as ease of use, value for money, pleasure and apps ranking. This is exceptionally true in the context of users downloading networking or social media type apps such as WhatsApp, WeChat, Twitter or Facebook. Concerning perceived behavioral control, ref [65] revealed that when smartphone users are given the choice to purchase premium apps that required the least permissions for personal data, they are more willing to purchase apps. While it is highlighted that these users may have high concern for information collection, they do have the ability to purchase expensive apps instead of just free apps. This shows that when users have high level of perceived behavioral control in the presence of personal data security, the intention of users to purchase smartphone apps will be higher.

## 7 Managerial Implications

The paper provides further insights to the knowledge concerning smartphone apps privacy concerns from the consumers' intention and attitude in Malaysia. This was done by investigating the concerns for information privacy dimensions. Some recommendations may be provided. Firstly, this study can assist the responsible government agencies in smartphone users' privacy security, concerns and consumer-related fields such as The Malaysian Communication and Multimedia Commission (MCMC). Privacy awareness campaigns should be more prevalent in the Malaysian context as it is confirmed that the privacy concerns in Asian countries such as Malaysia is low and worrying. Thus, this paper suggests that some guidelines and recommendations should be implemented to increase privacy awareness. These suggestions may include organizations maintaining solid security policies, assessing security awareness in regular periods, develop easy to access and understand information security learning sessions and establishing long term implementation to get users involved in security training. These recommendations, in hindsight can also be applied to the general public. As for the study's implication on the role of smartphone app stores administrators such as Google Play Store and Apple Store as well as smartphone app developers, the current policies and standards set forth by these parties with accountability may not be sufficient in ensuring safe and reliable information practices. It is recommended that certain actions to be considered for better data protection and integrity. Government may also intervene or act by asking app stores and developers to stop collecting smartphone users' personal information, investing in cybercrime and infrastructure and creating standard and guidelines for data collection in smartphone devices. Important government agencies such as MCMC may collaborate with foreign agencies to establish an intricate network of cooperation in sharing information and practices that can enhance security measures for the smartphone realm.

## 8 References

- [1] DMA. 2015. "Data privacy: what the customers really thinks," *Future Foundations*. Available at <https://dma.org.uk/research/data-privacy-2015-what-the-consumer-really-thinks>
- [2] Sheehan, K. B. and Hoy, M. G. 1999. "Flaming, complaining, abstaining: How online users respond to privacy concerns," *Journal of Advertising*, (28:3), pp. 37-51.
- [3] Cho, H., Rivera-Sanchez, M. and Lim, S. S. 2009. "A multinational study on online privacy concern: global concerns and local responses". *Journal of New Media and Society*, (11:3), pp. 395-416.
- [4] Malaysian Communication and Multimedia Commission (MCMC). 2014. *Statistical Brief Number Fourteen: Hand Phone Users Survey*.
- [5] Euromonitor International 2014. *Smartphone users do not pay for apps*. Retrieved 16 May 2014.

- [6] Thurm, S., & Kane, Y. I. 2010. "Apps Are Watching You: A WSJ Investigation Finds That iPhone and Android Apps Are Breaching the Privacy of Smartphone Users," *The Wall Street Journal*.
- [7] Angwin, J., & Valentino-Devries, J. 2011. "Apple, Google Collect User Data," *The Wall Street Journal*.
- [8] Al-Hadadi, M. and Al Shidhani, A. 2013. "Smartphone security awareness: Time to act," *Paper presented at Current Trends in Information Technology (CTIT)*, pp. 11-39. <https://doi.org/10.1109/CTIT.2013.6749496>
- [9] De Cristofaro, E. 2011. "Reclaiming privacy for smartphone apps," *Pervasive Computing and Communications (PerCom), 2011 IEEE International Conference*, pp. 84-92.
- [10] Dai, B. Forsythe, Sandra; and Wi-Suk Kwon. 2014. "The impact of online shopping experience on risk perceptions and online purchase intentions: Does product category matter?," *Journal of Electronic Commerce Research*, (15:1), pp. 13-24.
- [11] Lai, I. K. W., & Lai, D. C. F. 2014. "User acceptance of mobile commerce: An empirical study in Macau," *International Journal of Systems Science*, (45:6), pp. 1321-1331.
- [12] Khalifa M. and Shen, K. N. 2008. "Explaining the adoption of B2C mobile commerce," *Journal of Enterprise Information Management*, (21 :2), pp. 110-124.
- [13] Yang, K. 2012. "Consumer technology traits in determining mobile shopping adoption: An apps of the extended theory of planned behavior," *Journal of Retailing and Consumer Services*, (19:5), pp. 484-491.
- [14] Corlett, J. A. 2002. "The Nature and Value of the Moral Right to Privacy," *Public Affairs Quarterly*, (16:4), pp. 329-350.
- [15] Laudon, K. C., & Traver, C. 2001. *E-Commerce: Business, Technology, Society*. Boston, MA: Addison Wesley.
- [16] Sheng, N.H., Nah, F.-H., & Siau, K. 2008. An Experimental Study on Ubiquitous Commerce Adoption: Impact of Personalization and Privacy Concerns. *Journal of the Association for Information Systems*, (9:6), pp. 344-376.
- [17] Smith, H. J., S. J. Milberg, S. J. Burke. 1996. Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*. 20(2) 167-196 <https://doi.org/10.2307/249477>
- [18] Preibusch, S. 2013. "Guide to measuring privacy concern: Review of survey and observational instruments," *Int. J. Human-Computer Studies*, (71), pp. 1133-1143.
- [19] Stone, E.F., Gueutal, H.G., Gardner, D.G., and McClure, S., 1983. "A field experiment comparing information privacy values, beliefs, and attitudes across several types of organizations," *Journal of Applied Psychology*, (68:3), pp. 1983, 459.
- [20] Van Slyke, C., Shim, J. T., Johnson, R., & Jiang, J. J. 2006. "Concerns for Information Privacy and Online Consumer Purchasing. *Journal of the Association for Information Systems*," (7:6), pp. 415-444.
- [21] Stewart, K. A. and Segars, A. H. 2002. "An empirical examination of the concern for information privacy instrument," *Information System Research*, (13:1), pp. 36-49.
- [22] Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). "What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors," *Management Information Systems Quarterly*, (39:4), pp. 837-864.
- [23] Mylonas, A., Kastania, A. and Gritzalis, D. 2013. "Delegate the smartphone user security awareness," *Computers and Security*, (34), pp. 47-66. <https://doi.org/10.1016/j.cose.2012.11.004>
- [24] Felt, A. P., Egelman, S. and Wagner, D. 2012. "I've got 99 problems, but vibration ain't one: a survey of smartphone users' concerns," *SPSM '12: Proceedings of the second ACM*

- workshop on security and privacy in smartphones and mobile devices*, pp. 33-44. <https://doi.org/10.1145/2381934.2381943>
- [25] Gomez-Martin, L. 2012. "Smartphone usage and the need for consumer privacy laws," *Pittsburgh Journal of Technology and Policy*, (12:2), pp. 1-21.
- [26] Oreskovic, A. and Sin, M. 2013, Feb 14. *Google app store policy raises privacy concerns*. Retrieved 03 December 2013, from Reuters Official Website.
- [27] Smith, E. 2010. "iPhone applications and privacy issues: An analysis of application transmission of iPhone Unique Device Identifiers (UDID)," *Technical Report 2010*.
- [28] Painter, M. 2013, Nov 19. Fortify on Demand Mobile releases the HP Mobile Apps Security Vulnerability Report. Retrieved 03 December 2013, from HP Official Website.
- [29] Ajzen, I. 1985. "From intentions to actions: A theory of planned behavior," *Springer Series in Social Psychology*, pp. 11-39.
- [30] Ajzen, I. and Fishbein, M. 1980. *Understanding attitudes and predicting social behavior*, Englewood Cliffs, NJ: Prentice Hall.
- [31] Fishbein, M. and Ajzen, I. 1975. *Belief, attitude, intention and behavior: An introduction to theory and research*. Reading, MA: Addison-Wesley.
- [32] Ajzen, I. 1991. "The theory of planned behavior," *Organizational Behavior and Human Decision Process*, (50:2), pp. 179-211.
- [33] George, J. (2006). "The theory of planned behavior and Internet purchasing," *Internet Research*, (14:3), pp. 198-212.
- [34] Pavlou, P. and Fygenson, M. 2006. "Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior," *MIS Quarterly*, (30:1), pp. 115-143.
- [35] Davis, F. D. 1989. "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *Management Information Systems Quarterly*, (13:3), pp. 319-339.
- [36] Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. 2003. "User Acceptance of Information Technology: Toward a Unified View," *Management Information Systems Quarterly*, (27:3), 425-478.
- [37] Festinger, L. (1957). *A Theory of Cognitive Dissonance*. Stanford, CA: Stanford University Press.
- [38] Brown, M. and Muchira, R. 2004. "Investigating the relationship between Internet privacy concerns and online purchase behavior," *Journal of Electronic Commerce Research*, (5:1), pp. 62-70.
- [39] Liao, C., Liu, C. and Chen, K. 2011. "Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: An integrated model," *Electronic Commerce Research and Application*, 10: 702-715. <https://doi.org/10.1016/j.elerap.2011.07.003>
- [40] Korzaan, M. L., & Boswell, K. T. 2008. "The influence of personality traits and information privacy concern on behavioral intentions," *Journal of Computer Information Systems*, (4), pp. 15-24.
- [41] Cases, A., Fournier, C., Dubois, P. and Tanner Jr., J. 2010. "Web site spill over to e-mail campaigns: The role of privacy, trust and shoppers' attitudes," *Journal of Business Research*, (63:9-10), pp. 993-999.
- [42] Phelps, J., D'Souza, G. and Nowak, G. 2001. "Antecedents and consequences of consumer privacy concerns: An empirical investigation," *Journal of Interactive Marketing*, (15:4), pp. 2-17.
- [43] Chellappa, R. K., & Sin, R. G. 2005. "Personalization versus privacy: An empirical examination of the online consumer's dilemma," *Information Technology Management*, (6:2), pp. 181-202.

- [44] Zorotheos, A. and Kafeza, E. 2009. "Users' perceptions on privacy and their intention to transact online: a study on Greek internet users," *Direct Marketing: An International Journal*, (3:2), pp. 139-153.
- [45] Aldás-Manzano, J., Ruiz-Mafe, C. and Sanz-Blas, S. 2009. Exploring individual personality factors as drivers of m-shopping acceptance. *Industrial Management and Data Systems*, 109 (6): 739-757. <https://doi.org/10.1108/02635570910968018>
- [46] Cho, J. 2004. "Likelihood to abort online transaction: Influences from cognitive evaluations, attitudes, and behavioral variables," *Information and Management*, (41:7), pp. 827-838.
- [47] Sekaran, U. 2003. *Research Methods for Business: A Skill Building Approach* (4th ed.). NY: John Wiley and Sons, Inc.
- [48] Preacher, K. J., & Hayes, A. F. (2004). SPSS and SAS procedures for estimating indirect effects in simple mediation models. *Behavior Research Methods, Instruments, and Computers*, 36, 717-731. <https://doi.org/10.3758/BF03206553>
- [49] Rivera, M., Gregory, A., Cobos, L., (2015) "Mobile application for the timeshare industry: The influence of technology experience, usefulness, and attitude on behavioral intentions", *Journal of Hospitality and Tourism Technology*, (6:3), pp.242-257. <https://doi.org/10.1108/JHTT-01-2015-0002>
- [50] Korzaan, M., Brooks, N., & Greer, T. 2009. "Demystifying personality and privacy: An empirical investigation into antecedents of concern for information privacy," *Journal of Behavioral Studies in Business*, 1, 1–17.
- [51] Osatuyi, B. 2015. "Personality Traits and Information Privacy Concerns on Social Media Platforms," *Journal of Computer Information Systems*, (55:4), pp. 11–19.
- [52] Eagly, A. H., & Chaiken, S. 1993. *The Psychology of Attitudes*. Orlando, FL: Harcourt Brace Javanovich, Inc.
- [53] Culnan, M. J. 1995. "Consumer awareness of name removal procedures: Implication for direct marketing," *Journal of Interactive Marketing*, (9:2), pp. 10-19.
- [54] Angst, C., M. and Agarwal, R. 2009. "Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion," *MIS Quarterly*, (33: 2) pp.339-370.
- [55] Culnan, M. J.(1993). 'How did they get my name?' An exploratory investigation of consumer attitudes toward secondary information use, *MIS Quarterly*, (17: 3), pp 341-364.
- [56] Chin, W. W. 1998. "Issues and opinions on structural equation modelling," *Management Information Systems Quarterly*, (21:1), pp. 7-16.
- [57] Kumar, N., Mohan, K. and Holowczak, R. 2008. "Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls," *Decision Support Systems*, (46:1), pp. 254-264.
- [58] Nguyen, D. H., Bedford, A., Bretana, A., & Hayes, G. R. 2011. "Situating the Concerns for Information Privacy through an Empirical Study of Responses to Video Recording," *Paper presented at the SIGCHI Conference on Human Factors in Computing Systems (CHI '11)*. <https://doi.org/10.1145/1978942.1979419>
- [59] Bellman, S., Johnson, E. J., Kobrin, S. J., & Lohse, G. L. 2004. "International Differences in Information Privacy Concerns: A Global Survey of Consumers," *The Information Society*, (20:5), pp. 313–324.
- [60] Rose, E. (2016) An examination of the concern for information privacy in the New Zealand regulatory context. *Information & Management*, Volume 43, Issue 3, pp 322–335.
- [61] Malhotra, N. K., Kim, S. and Agarwal, J. 2004. "Internet users' information privacy concerns (IUIPC): The construct, the scale and a causal model," *Information System Research*, (15:4), pp. 336-355.

- [62] Xu, H., Gupta, S., Rosson, M. B. and Carroll, J. 2012. "Measuring mobile users' concerns for information privacy," *Paper presented at the 33<sup>rd</sup> International Conference on Information System*.
- [63] Yusliza, M. Y. and Ramayah, T. 2011. "Explaining the intention to use electronic HRM among HR professional: Results from a pilot study," *Australian Journal of Basic and Applied Sciences*, (5:8), pp. 489-497.
- [64] Kim, H., Lee, H. L. and Son, J. E. 2011. "An exploratory study on the determinants of smartphone app purchase," *Paper presented at the 11<sup>th</sup> International DSI and the 16<sup>th</sup> APDSI Joint Meeting on 11<sup>th</sup>-26<sup>th</sup> July 2011*.
- [65] Egelman, S., Felt, A. P. and Wagner, D. 2013. "Choice architecture and smartphone privacy: There's a price for that," *The Economics of Information Security and Privacy*, pp. 211-236.

## 9 Authors

**Zakariya Belkhamza (corresponding author)** is a senior lecturer of management information systems at the Faculty of Business, Economics and Accountancy, Universiti Malaysia Sabah, where he teaches management information systems subjects at both undergraduate and postgraduate level. His research interests include IT management, IS implementation and evaluation, Mobile technologies management. He authored and edited two books in the field of Management Information systems, in addition to various research and publications ([zakariya@ums.edu.my](mailto:zakariya@ums.edu.my)).

**Mohd Adzwin Faris** is a doctorate candidate at the Faculty of Business, Economics and Accountancy, Universiti Malaysia Sabah. He obtained his Master's Degree in Business Administration from Universiti Malaysia Sabah in 2014. He has prior experience in the financial service industry for more than 3 years. His research interests include management information system, digital marketing, mobile-based activities / behaviors and e-commerce.

Article submitted 29 March 2017. Published as resubmitted by the authors 14 May 2017.