Computers in Human Behavior 91 (2019) 167–185

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

Understanding users' willingness to put their personal information on the personal cloud-based storage applications: An empirical study

Andree E. Widjaja[a], Jengchung Victor Chen[b], Badri Munir Sukoco[c], Quang-An Ha[b,*]

[a] Department of Information Systems, School of Information Science and Technology, Pelita Harapan University, Indonesia
[b] Institute of International Management, National Cheng Kung University, No.1.University Road, Tainan City, Taiwan
[c] Department of Management, Faculty of Economics and Business, Airlangga University, Indonesia

ARTICLE INFO

Keywords:
Privacy
Cloud storage
Communication privacy management theory
Privacy-trust-behavioral intention model
Information sensitivity
Culture

ABSTRACT

Despite prevalent privacy and security threats on the cloud, users have put tremendous amounts of their personal information on cloud storage. This present study proposes a comprehensive research framework to investigate cloud storage users' willingness to put personal information on personal cloud-based storage applications. Our research framework is theoretically derived from the Communication Privacy Management Theory and Privacy-Trust-Behavioral Intention Model. To empirically test our research framework, we conducted an online survey of 786 active cloud storage users both in Indonesia and Taiwan. The findings suggest that cloud storage users' willingness to put personal information is highly influenced by trust, perceived costs, perceived benefits, and also the degree of sensitivity of the personal information. Some findings with regard to cultural differences between the two countries are also showed out. The key findings, implications, and limitations are discussed in this paper.

1. Introduction

Cloud storage has been widely used as online storage virtualization by many people in around the globe. As in 2018, cloud storage users have reached around 1.926 billion users (Statista, 2018) and up to now tremendous amount of data has been put onto the cloud, including the sensitive one (Kohgadai, 2018). However, since the data is digitally recorded on the cloud, users may lose control over their data, and consequently, privacy and security concerns, as well as privacy risks may be raised. Users may not exactly know what will happen to their data, and whether cloud storage providers will keep their data safe or use it for their own benefits.

Privacy and security issues on the cloud storage have been tremendous problems (Chou, 2013; Kalloniatis et al., 2014). For example, in 2014, iCloud was breached by hackers (Lewis, 2014). Other incidents of security weaknesses as well as cyber attacks on Google Drive, Dropbox, and Amazon Web Services cloud storage server had also been reported (Chou, 2013; Chu et al., 2013; Johnson, 2018). Moreover, some surveys also showed that users have high privacy and security concerns on cloud storage (Barker, 2015; Gasiorowski-Denis, 2015). Thus, in light of the pertinent cloud storage privacy and security issues, and the amount of data that users have put on the cloud, cloud storage privacy and security related research should be of utmost importance.

To dates, there is a large number of prior works examining cloud storage that focus on the technical sides, e.g., (Du, Wang, & He, 2018; Wu, Chen, Zeadally, & He, 2018). Nevertheless, there is only a handful of studies exploring the use of cloud storage from the perspective of its end users. Such studies e.g., (Arpaci, 2016; Ghaffari & Lagzian, 2018; Menard, Gatlin, & Warkentin, 2014; Wu, Vassileva, & Zhao, 2017; Yang & Lin, 2015) can be found in the literature; however, most of them were mostly focused on investigating user intention or experience related to the use of cloud storage, and thus they did not distinctively center their research on the privacy and security related issues. While there is a few recent studies addressing privacy and security in cloud storage e.g., (Alsmadi & Prybutok, 2018; Li, Chang, & Wang, 2017), still little is known about the privacy and security related factors that cause users' willingness to put their personal information onto cloud storage, the influence of culture, and the role of information sensitivity within cloud storage for personal use context.

This study therefore aims to address cloud storage privacy and security issues in a more comprehensive manner in which it is explicitly directed toward investigating users' willingness to put their personal information onto cloud storage. To better examine the complexities of privacy and security related constructs, this study is guided by

* Corresponding author.
E-mail addresses: andree.widjaja@uph.edu (A.E. Widjaja), victor@mail.ncku.edu.tw (J.V. Chen), badri@feb.unair.ac.id (B.M. Sukoco), RA8047011@mail.ncku.edu.tw (Q.-A. Ha).

https://doi.org/10.1016/j.chb.2018.09.034
Received 18 June 2018; Received in revised form 5 September 2018; Accepted 24 September 2018
Available online 26 September 2018

theoretical lens of the Communication Privacy Management Theory, the Privacy-Trust-Behavioral Intention Model, Hofstede's Cultural Dimensions, and Information Sensitivity. Drawing from the aforementioned theories and through a research framework that we develop, we aim to answer the following research questions:

(1) Drawing from the Communication Privacy Management Theory and the Privacy Trust Behavioral intention model, what are the significant factors affecting users' willingness to put personal information onto cloud storage?
(2) Does culture affect some of the relationships among the factors proposed in the research framework?
(3) Do different levels of information sensitivity (more sensitive vs. Less sensitive personal information) make any difference in the relationships among perceived cost, trust, and users' willingness to put personal information on the cloud storage?

2. Theoretical framework

2.1. Personal Cloud-Based Applications

A Personal Cloud-Based Application (PCBA) is a type of cloud computing service under application-*as*-a-service category in which the cloud provider provides some personal applications that can be accessed by individual users via web browsers or specific applications (Forrester, 2012; Wu et al., 2017). This study specifically focuses on PCBA such as Google Drive, Microsoft One Drive, Drop Box, and others for online data backup and storage. Meanwhile, with regard to different types of data, Forester research (2012) described at least four different types of personal information that individuals most commonly put onto online internet services (e.g., cloud storage): 1) media (e.g. videos and music), 2) work documents (e.g. word, excel files, PDFs, contacts, and calendars), 3) photos and personal documents, and 4) personal identity or financial information (e.g. driver's license, passport, birth certificate, social security number, tax returns, banking or credit card information).

2.2. Communication Privacy Management Theory (CPMT)

CPMT is a communication theory that was originally developed to examine how individuals make decisions to disclose personal information within interpersonal relationships (Petronio, 2002; Xu, Dinev, Smith, & Hart, 2011). CPMT depends on the notion of a boundary metaphor for conceptualizing the process of privacy management (Petronio & Durham, 2008), and the theory has three important main elements, namely: privacy ownership, privacy control, and privacy turbulence (please refer to Petronio (2013), Child, Haridakis, and Petronio (2012), and Petronio (2002) for comprehensive reviews of CPMT). These aforementioned elements were argued to be evident in online privacy management (Metzger, 2007; Xu et al., 2011). To date, this theory has been developed to explain disclosure behavior in various settings, including its applicability to privacy issues generated by new technologies (Metzger, 2007).

This study is specifically guided by CPMT as it was applied in Xu et al. (2011) study. In Xu et al. (2011), boundary coordination and boundary turbulence are represented by institutional privacy assurances. Meanwhile, boundary rule formation is represented by privacy control, perceived risk, and disposition to privacy. Their final dependent variable was privacy concern within the context of four different types of online websites. In this study, we applied CPMT within the context of cloud storage for personal use. As this study solely focuses on the cloud storage context, we therefore excluded “context” privacy rule criteria as mentioned in Xu et al. (2011). In addition, we integrated the Privacy-Trust-Behavioral Intention Model into our research framework to better answer our research questions.

2.3. Privacy-trust –behavioral intention model

The Privacy-Trust-Behavioral Intention model was proposed by Liu, Marchewka, Lu, and Yu (2005) to explain how privacy affects trust and how trust affects behavioral intention within e-commerce environments. In the model, privacy is argued as the major antecedent of trust. Wu, Huang, Yen, and Popova (2012) adapted this model to study the effect of privacy policy on privacy concern and trust within the general online websites context. Since trust has been regarded as a critical component in the cloud computing environment (King & Raja, 2012), it is thus reasonable to incorporate trust as a construct in our research framework and to link it with CPMT. This study research framework is illustrated in Fig. 1.

3. Research variables and hypotheses development

3.1. Willingness to put personal information

In this study, we aim to investigate users' willingness to put their personal information onto cloud storage. Users' behavioral willingness, as mentioned by Gibbons and Gerrard (1995), will reflect an individuals' openness to perform a specific behavior depending on the circumstances or the situation. Based on Forrester (2012), we propose a new construct that includes five different types of personal information that may be put onto cloud storage (i.e. work related documents, personal media, personal documents, personal identity information, and specific sensitive information). This construct is therefore defined as a user's general willingness to put personal information onto cloud storage. By referring to the degree of information sensitivity as defined in Smith, Dinev, and Xu (2011), these five types of personal information are divided into two categories: less sensitive personal information and more sensitive personal information. The construct and final dependent variables of this study are then labeled as “Willingness to Put Less Sensitive Personal Information” and “Willingness to Put More Sensitive Personal Information”.

3.2. Trust

Information Systems (IS) literature shows that trust is usually viewed as a strong predictor of behavior (Slyke, Shim, Johnson, & Jiang, 2006). In our study, trust refers to trusting beliefs (McKnight, Choudhury, & Kacmar, 2002), and it is defined as a user's overall trust in a cloud storage provider related to delivering trusted services. Trust in a cloud storage provider may be uncertain for many reasons. One of the major reasons is related to user concerns related to information security and privacy, which may negatively affect their willingness to use cloud storage. However, when users believe that a cloud storage provider is able to deliver trusted services, they will be more likely to have higher willingness to put their personal information onto cloud storage. Thus, the following hypotheses are posited:

Hypothesis 1a. Trust will positively affect users' willingness to put less sensitive personal information.

Hypothesis 1b. Trust will positively affect users' willingness to put more sensitive personal information.

3.3. Boundary rule formation

CPMT posits that people use privacy rules to decide whether to open (disclose personal information) or close privacy boundaries (conceal personal information). Moreover, CPMT also posits cost and benefits are part of a rule-based management system and are part of the catalyst of privacy rule criteria (Petronio, 2013). By considering numerous related IS literature, e.g., (Chou, 2013; Dinev & Hart, 2006; Jiang, Heng, & Choi, 2013; Keith, Thompson, Hale, Lowry, & Greer, 2013; Krasnova,

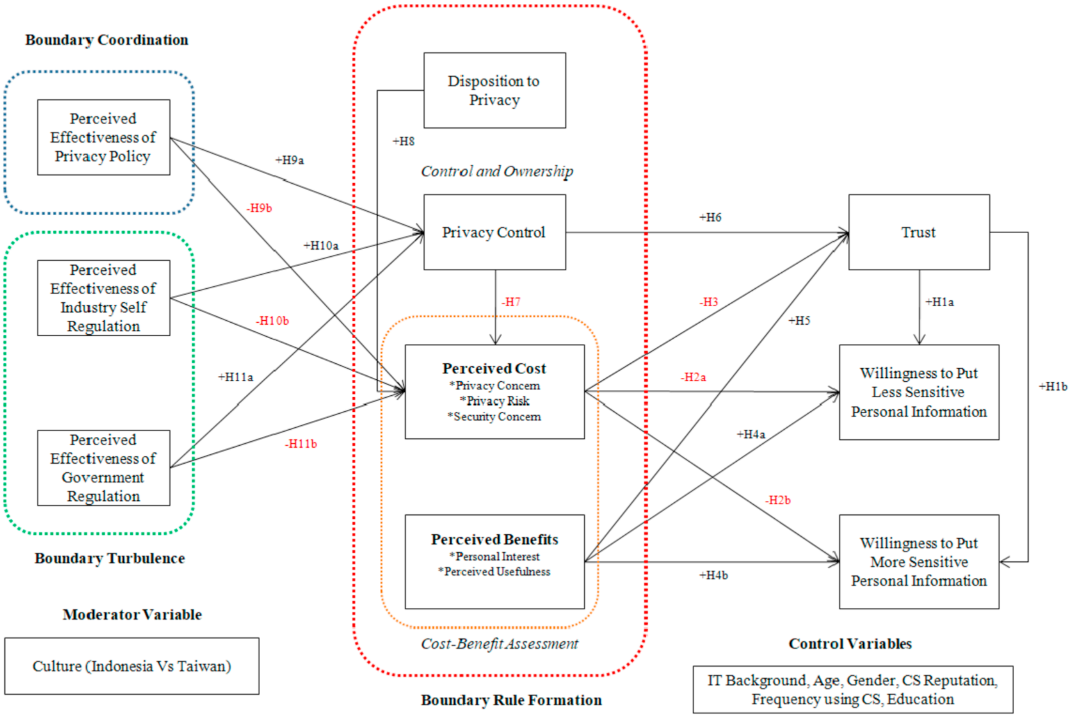

Fig. 1. Research framework.

Veltri, & Günther, 2012; Yang & Lin, 2015), we decided to operationalize perceived cost as a second order construct that consists of privacy concerns, privacy risk, and security concerns. Meanwhile, perceived benefits are also operationalized as a second order construct comprising personal interest and perceived usefulness.

Privacy concerns refers to the specific concerns that reflect users' inherent worries about possible loss of information privacy when putting their personal information onto cloud storage (Xu et al., 2011). Privacy risk is defined as the expectation of loss associated with putting personal information onto cloud storage (Xu, Teo, Tan, & Agarwal, 2009). Security concerns are associated to the specific concerns that reflect users' inherent worries about possible security and safety issues when putting their personal information onto cloud storage (Nepomuceno, Laroche, & Richard, 2014). Thus, due to the negative effect of privacy concerns, privacy risk, and security concerns on users' willingness as well as trust, it can be hypothesized that:

Hypothesis 2a. Perceived cost will negatively affect users' willingness to put less sensitive personal information.

Hypothesis 2b. Perceived cost will negatively affect users' willingness to put more sensitive personal information.

Hypothesis 3. Perceived cost will negatively affect trust.

Meanwhile, personal interest is defined as the degree of cognitive attraction to users related to obtaining and using the personal information that they put onto cloud storage (Dinev & Hart, 2006). Perceived usefulness in this study refers to the perceived usefulness of putting personal information onto cloud storage (Gefen, Karahanna, & Straub, 2003). Thus, perceived benefits which consist of both personal interest and perceived usefulness might have positive effect on users' willingness as well as trust, in so doing we expect that:

Hypothesis 4a. Perceived benefits will positively affect users' willingness to put less sensitive personal information.

Hypothesis 4b. Perceived benefits will positively affect users' willingness to put more sensitive personal information.

Hypothesis 5. Perceived benefits will positively affect trust.

CMPT posits that individuals should be able to control and be the owners of their private information (Petronio & Durham, 2008). In this study, privacy control refers to users' subjective perception and beliefs in their ability to control the personal information that is recorded when using cloud storage and how cloud storage providers will use their personal information (Dinev & Hart, 2004). Users' control over their privacy might have a positive effect on trust, however if such control is lost, it might have a negative effect on perceived cost. Hence, we propose that:

Hypothesis 6. Privacy control will positively affect trust.

Hypothesis 7. Privacy control will negatively affect perceived cost.

CPMT includes individual privacy orientation in terms of boundary rule formation (Petronio & Durham, 2008). We argue that disposition to a privacy (DTP) construct is similar to the privacy orientation notion, as mentioned in CPMT. According to Xu et al. (2011), DTP is defined as "an individual's general tendency to preserve his or her personal information space or to restrain disclosure of personal information across a broad spectrum of situations and contexts" (p. 805). When using cloud storage, users with higher DTP will value privacy more, so they may perceive higher risks and may have higher privacy and security-related concerns as compared to those with lower DTP, thus the following hypothesis is proposed:

Hypothesis 8. Disposition to privacy will positively affect perceived cost.

3.4. Boundary coordination

CPMT suggests that after individuals disclose private information to other people, these people will then become the co-owners of their private information (Petronio & Durham, 2008). Consequently, both owner and co-owner have to coordinate by making sure that they keep the information private. In this study, we define perceived effectiveness of privacy policies as the extent to which users believe in the accuracy, reliability, and comprehensiveness of a cloud storage provider's privacy practices as written in their privacy policy (Xu et al., 2011). Previous studies have found that when a firm states its privacy policy, it will reduce consumers' perceived risk (Culnan & Amstrong, 1999) and increase consumers' perceived privacy control (Milne & Culnan, 2004). Accordingly, we argue that high perceived effectiveness of a privacy policy can have a positive impact on privacy control and a negative impact on perceived cost. Based on the aforementioned argument, we expect that:

Hypothesis 9a. Perceived effectiveness of a privacy policy will positively affect privacy control.

Hypothesis 9b. Perceived effectiveness of a privacy policy will negatively affect perceived cost.

3.5. *Boundary turbulence*

According to CPMT, boundary coordination may not work properly due to its complexity and thus can cause privacy turbulence (Petronio & Durham, 2008). Drawing from an institutionally-based trust concept (McKnight et al., 2002), when there is a case of privacy violation, individuals can rely on third party institutions to independently assure their privacy rights. Thus, industry self-regulatory programs as another form of institutional privacy assurance are often implemented by online companies. There are various industry groups (e.g., Cloud Security Alliance) and certifying institutions (e.g., TRUSTe Cloud Privacy Certification) attempting to independently assure privacy practices specifically in the cloud computing environment.

In this study, perceived effectiveness of industry self-regulation is defined as the extent to which users believe that independent cloud computing policing industry groups as well as certifying agencies are capable of objectively safe-guarding their online privacy when they are using cloud storage (Xu et al., 2011). Prior studies have examined the effectiveness of privacy seals on e-commerce websites and location-based services in regard to assuring user privacy, e.g. (Hui, Teo, & Lee, 2007; Xu et al., 2009). Hence, we argue that effective industry self-regulation may enhance user's perceived control and reduce perceived cost. The following hypothesis is proposed:

Hypothesis 10a. Perceived effectiveness of industry self-regulation will positively affect privacy control.

Hypothesis 10b. Perceived effectiveness of industry self-regulation will negatively affect perceived cost.

In a turbulent environment, especially when a cloud storage institution and industry self-regulation cannot fully assure users' privacy needs, government regulations can provide redress to users who are harmed due to the privacy violations. Previous privacy-related studies mentioned that government legislation is one of the major and most commonly used approaches to protecting information privacy (Culnan & Bies, 2003; King & Raja, 2012; Xu, Teo, Tan, & Agarwal, 2010).

Each country has its own specific government regulations and laws to protect its citizens' personal information whether online or offline or both. For example, Taiwan passed the Personal Data Protection Law in 2010 (Piper, 2013). Meanwhile, Indonesia issued the Provision of Electronic System and Transaction in 2012 (Piper, 2013). These government regulations to some extent may cover some privacy and security-related issues in the cloud computing environment. However, not all citizens in the country will believe that their government regulations can really protect them (Chiou, Chen, & Bisset, 2007). We therefore argue that the effectiveness of government regulations may have an impact on users' subjective perceptions with regard to their perceived privacy costs as well as their perceived privacy control related to using cloud storage. Hence, it is expected that:

Hypothesis 11a. Perceived effectiveness of government regulation will positively affect privacy control.

Hypothesis 11b. Perceived effectiveness of government regulation will negatively affect perceived cost.

3.6. *The influence of culture*

The significant role of culture has been postulated in CPMT as one of the cores privacy values which concerns how cultural expectations influence the level of privacy and information disclosure (Petronio & Durham, 2008). Prior literature also suggested that different countries differ with regard to their degree of concern over privacy (Krasnova et al., 2012). To address cultural issue, a large body of previous works e.g., (Cockcroft & Rekker, 2015; Krasnova et al., 2012; Leidner & Kayworth, 2006; Lowry, Cao, & Everard, 2011; Ng, 2013) generally applied Hofstede (2001) cultural dimensions framework in which the culture can be divided into five dimensions (please refer to Hofstede (2011), Hofstede (2001), and Hofstede (1991) for more detailed explanations regarding Hofstede's cultural dimensions).

In this study, we included two cultural dimensions that are relevant within the context of our study (a comparison of two countries – Indonesia and Taiwan), namely Uncertainty Avoidance (UA) and Power Distance (PD). UA refers to the degree to which societies feel uncomfortable and threatened with uncertainty, ambiguity, or unknown situations, whereas PD refers to equal or unequal power distribution in the society (Hofstede, 1991). We operationalized these two cultural dimensions aforementioned at the national level. The comparison is based on the established Hofstede's cultural dimension scores as published on Hofstede's website (http://geert-hofstede.com/countries.html) which state that Indonesia scores lower (48) on the UA dimension as compared to Taiwan (69). Meanwhile, Indonesia has a higher score (78) on the PD dimension as compared to Taiwan (58). By referring to prior works e.g., (Bellman, Johnson, & Kobrin, 2004; Cao & Everard, 2008; Cockcroft & Rekker, 2015; Lowry et al., 2011; Yoon, 2009), UA might be related to privacy concern, control, laws and regulation, and trust. Meanwhile, PD might be related to privacy concern. The cultural related hypotheses are the followings:

H12a. Culture, as differentiated by UA dimension, will moderate the relationship between perceived effectiveness of government regulation and privacy control, such that high UA culture (Taiwan) will have a stronger positive relationship than low UA culture (Indonesia).

H12b. Culture, as differentiated by UA dimension, will moderate the relationship between trust and users' willingness to put less sensitive personal information in the cloud storage, such that high UA culture (Taiwan) will have a stronger positive relationship than low UA culture (Indonesia).

H12c. Culture, as differentiated by UA dimension, will moderate the relationship between trust and users' willingness to put more sensitive personal information in the cloud storage, such that high UA culture (Taiwan) will have a stronger positive relationship than low UA culture (Indonesia).

3.7. *Information sensitivity*

Information sensitivity is defined as “the level of privacy concern an individual feels for a type of data in a specific situation,” p.10 (Weible, 1993). More sensitive information will be perceived as riskier and more uncomfortable to reveal (Cranor, Reagle, & Ackerman, 1999). Several researchers have demonstrated that the individuals will show higher concern about requests for specific types of personal information such as medical records, social security numbers, and financial information (Nowak & Phelps, 1997; Sheehan & Hoy, 2000; Ward, Bridges, & Chitty, 2005; Yang & Wang, 2009). All of these more sensitive types of personal information can be put onto cloud storage. It is expected that, due to the higher perceived cost, more sensitive information will cause lower levels of willingness for consumers to provide such information (D'Souza & Phelps, 2009). We therefore propose the following hypothesis:

Hypothesis 13a. The relationship between perceived cost and users' willingness to put more sensitive personal information will be negatively stronger than the relationship between perceived cost and users' willingness to put less sensitive personal information.

Information sensitivity is argued to be associated with trust (Bansal, Zahedi, & Gefen, 2010). Bansal, Zahedi, and Gefen (2015) further argued that in a more highly sensitive context, the presence of trust is even more critical in terms of disclosing private information online. This means that trust will be more important and required for users when they are disclosing highly sensitive personal information online as compared to when they are sharing less sensitive personal information. Thus, we propose the following hypothesis:

Hypothesis 13b. The relationship between trust and users' willingness to put more sensitive personal information will be positively stronger than the relationship between trust and users' willingness to put less sensitive personal information.

3.8. Control variables

CPMT has acknowledged the role of gender in its theoretical framework (Petronio & Durham, 2008). Gender has been found to affect privacy-related issues. For instance, Hew (2011) indicated that gender can predict information disclosure such that females spend more time on Facebook have greater privacy restrictions on their profiles than males. We thus included gender as one of the control variables in our research framework. Meanwhile, In the online environment, the reputation of a website has been studied as a contextual factor that will negatively influence website-specific privacy concerns (Li, 2014), hence the reputation of cloud storage can also serve as control variable. In addition to gender and reputation, we also included age, education, IT background, and frequency of using cloud storage as control variables.

4. Research methodology

4.1. Sample and data collection procedure

Indonesia and Taiwan were chosen as the sample for this study. There are three main reasons for this selection. First, there is a significant difference between Indonesia and Taiwan with regard to Hoftstede's cultural dimension (the UA and PD dimensions). UA plays an important role in various IS related studies. Second, Indonesia is considered to be a developing country, whereas Taiwan is considered to be a more developed country. Due to the difference in terms of technology adoption and infrastructure, we argue that users who live in a developed country such as Taiwan might perceive online information privacy issues differently than those users who live in a less developed country such as Indonesia. The comparison between Indonesia and Taiwan can be important, particularly to shed light to Indonesia on how to further improve their technology capabilities in light of online privacy and security issues. Third, although both Indonesia and Taiwan have government regulations pertaining to online personal information protection, the actual effectiveness as well as the contribution or the effect of these laws in protecting their citizens' online information privacy might also be perceived differently by the citizens.

With regard to the data collection procedure, we collected the survey data using an online survey method in both countries. The target respondents were required to be active users of personal cloud-based storage applications. We used screening question such as “Are you currently using personal cloud-based storage such as Dropbox, Google Drive, Microsoft One Drive, or other similar services for personal use?” Those who answered “no” were not allowed to participate in the survey. The survey questionnaire items were carefully translated from English to Indonesian and Chinese using a back translation method. Small scale pilot tests (15 respondents) were conducted to test the accuracy of the English, Indonesian, and Chinese questionnaire. Based on the pilot test results and some valuable suggestions and recommendations from the pilot test respondents, we revised our survey measurements.

Finally, we collected the survey data using both convenience and snowballing sampling methods. We posted our online survey invitations in both countries (Indonesia and Taiwan) via social networking sites such as Facebook groups or forum, Facebook walls, Facebook events, personal instant-messages (e.g., Facebook messenger, LINE), and personal e-mails (Yahoo and Gmail). The researcher's personal instant messaging and Facebook account were mainly used to distribute the online survey invitations. We mentioned in our invitation that the respondents might also distribute our online survey to other people who were also cloud storage users. In total, we received 418 responses for the Indonesia sample and 439 responses for the Taiwan sample. After data cleaning, there were 383 usable responses for the Indonesian sample and 403 usable responses for the Taiwan sample. There were a total of 786 usable combined samples. Table 1 shows the demographic data of our respondents.

4.2. Measurement items

In this study, the majority of the measurement items were adapted from previous studies and modified to better fit the study context. All items were measured on 7 point Likert scales (strongly disagree – strongly agree, unless stated otherwise). The complete measurement items used in this study is reported in Appendix A.

4.3. Partial least square structural equation modeling (PLS SEM)

In this study, we used the SmartPLS 3.0 to analyze our data (Ringle, Sven, & Jan-Michael, 2015). We compared the two samples (Indonesia and Taiwan) based on the cultural differences dimensions (UA and PD). We combined the two samples in the data analysis for four main reasons. First, both samples consist of active cloud storage users who have been using cloud storage applications, and therefore it is likely that they have put their personal information onto cloud storage. Second, most proposed research constructs in this study are related and relevant for both samples. For example, the users in both samples may be concerned about privacy and security. Both countries do have government regulations related to online personal data protection; hence, perceived effectiveness of the government regulation construct is also related and relevant for both samples.

The combined samples, referring to the first and second reason, would thus be useful for the generalization of this study's results and findings. In addition, because worldwide cloud storage users comprise a diverse group, a larger sample size and more varied demographics (age, occupation, experience, etc.) may be needed in the data analysis to better represent the cloud storage users' actual population. Third, both samples also share some similar cultural dimensions. According to Hofstede's cultural dimension scores, both Indonesia and Taiwan are collectivist and feminine societies. The similar scores of the aforementioned cultural dimension may become one of the reasons for combining both samples in the data analysis. Lastly, combined samples are needed to run a Partial Least Square Multi Group Analysis (PLS MGA) using SmartPLS 3.0.

5. Research results

5.1. Descriptive statistics, PLS SEM confirmatory factor analysis (CFA) results

CFA was performed using the PLS algorithm in SmartPLS 3.0. With regard to PLS CFA factor loading rule of thumb, Hair, Ringle, and

Table 1
Demographics.

	Combined N = 786		Indonesia N = 383		Taiwan N = 403	
	#	%	#	%	#	%
Gender						
Male	472	60.1	230	60.1	242	60
Female	314	39.9	153	39.9	161	40
Age						
< =19 years old	76	9.7	9	2.3	67	16.6
20–25 years old	213	27.1	148	38.6	65	16.1
26–31 years old	195	24.8	129	33.7	66	16.4
32–37 years old	131	16.7	57	14.9	74	18.4
38–43 years old	89	11.3	26	6.8	63	15.6
44–49 years old	49	6.2	12	3.1	37	9.2
> 50 years old	33	4.2	2	0.5	31	7.7
Highest Education						
High school	71	9	50	13.1	21	5.2
Vocational/Diploma	48	6.1	1	0.3	47	11.7
Bachelor	399	50.5	191	49.9	208	51.6
Master	253	32.2	126	32.9	127	31.5
Doctoral	15	1.9	15	3.9	0	0
Occupation						
None/Not Working	5	0.6	5	1.3	0	0
Student	225	28.6	129	33.7	96	23.8
Public/Government Employees	74	9.4	25	6.5	49	12.2
Private Company Employees	403	51.3	152	39.7	251	62.3
Entrepreneur/Freelancer	46	5.9	39	10.2	7	1.7
Lecturer/Professor	33	4.2	33	8.6	0	0
IT Background						
None	396	50.4	122	31.9	274	68
Yes	390	49.6	261	68.1	129	32
Frequency Using Cloud Storage Application						
Seldom	146	18.6	13	3.4	133	33
Occasionally	88	11.2	35	9.1	53	13.2
Sometimes	115	14.6	68	17.8	47	11.7
Often	95	12.1	48	12.5	47	11.7
Frequently	129	16.4	86	22.5	43	10.7
Usually	119	15.1	77	20.1	42	10.4
Always	94	12	56	14.6	38	9.4
Most Used Cloud Storage Application						
Dropbox	174	22.1	104	27.2	70	17.4
Google Drive	427	54.3	259	67.6	168	41.7
HiCloud	61	7.8	0	0	61	15.1
iCloud	49	5.5	12	3.1	31	7.7
Microsoft One Drive	69	8.8	8	2.1	61	15.1
Other	12	1.5	0		12	3

Marko (2011) recommended the standardized indicator loadings should be higher than 0.70. There are three general indicators used to assess the construct reliability and convergent validity of a construct in PLS CFA, namely Composite Reliability (C.R.), Average Variance Extracted (AVE), and Cronbach's Alpha (α) (Wilson, 2010). Fornell and Larcker (1981) suggested a CR of 0.70 or greater is considered acceptable for research. AVE is suggested to be greater than 0.50 (Chin, 1998a). Meanwhile, Cronbach's α of 0.70 or greater is considered acceptable for research (Nunally, 1978). Nevertheless, CR value has been considered as a better indicator of the uni-dimensionality of a block than the Cronbach's alpha (Chin, 1998b). Raykov (2001) argued Cronbach's alpha is only reported as a matter of convention and should not be given much credence as it is the lower bound estimate of reliability. Besides, according to Malhotra and Dash (2011), CR alone can be used to measure the adequacy of Convergent Validity of a construct.

We proposed two constructs (perceived cost and perceived benefit) as the second order formative factors. First, perceived cost which consists of privacy concern, security concern and privacy risk. Second, perceived benefit consists of personal interest and perceived usefulness. We ran the PLS CFA analysis and reported the factor loading, AVE, CR, Alpha, Outer VIF values. Meanwhile, in the PLS second order formative data analysis (path coefficient analysis), we followed Lowry and Gaskin (2014) with regard to second order formative two steps analysis approach using latent variable scores known as "*repeated indicator approach*". Table 2 shows the descriptive statistics and PLS CFA results for combined sample (for sub sample – Indonesia and Taiwan PLS CFA results please see Appendix B). Meanwhile, the correlation table can be seen in Appendix C.

5.2. Common method variance

Since this study employed a single cross-sectional survey method, Common Method Variance (CMV) might be an issue. Therefore, two indicators were used to test the CMV to ensure our data validity and quality. First, a Harman's one-factor test was employed (Podsakoff, Mackenzie, Lee, & Podsakoff, 2003). The result showed that the largest factor explained 28.287% of the covariance for the combined data (25.046% for the Indonesian sample and 30.421% for the Taiwanese sample), indicating that CMV is unlikely to be a very serious problem. CMV will be a serious issue if the largest factor explained is higher than

Table 2
Descriptive statistics and PLS-CFA results for combined sample (second order formative).

Combined Sample N = 786

First Order Constructs	Mean	SD	Outer VIF Values	Factor Loading	AVE	C.R.	Cronbach's Alpha
Perceived Effectiveness of Privacy Policy					**0.850**	**0.944**	**0.912**
PEPP1	4.122	1.593	2.885	0.910			
PEPP2	4.058	1.587	3.234	0.931			
PEPP3	4.229	1.672	3.234	0.924			
Perceived Effectiveness of Industry Self-Regulation					**0.838**	**0.940**	**0.904**
PEISR1	4.141	1.632	2.513	0.887			
PEISR2	4.203	1.553	3.644	0.936			
PEISR3	3.952	1.534	3.048	0.924			
Perceived Effectiveness of Government Regulation					**0.848**	**0.944**	**0.910**
PEGRL1	3.671	1.679	2.528	0.891			
PEGRL2	3.436	1.639	4.909	0.953			
PEGRL3	3.268	1.648	3.679	0.918			
Privacy Control					**0.810**	**0.928**	**0.883**
C1	4.297	1.644	2.156	0.884			
C2	4.124	1.620	2.739	0.904			
C3	4.122	1.602	2.811	0.912			
C4	Deleted						
Privacy Risk					**0.817**	**0.947**	**0.925**
R1	4.421	1.776	3.246	0.897			
R2	4.713	1.701	4.339	0.929			
R3	4.620	1.764	4.056	0.923			
R4	4.749	1.733	2.614	0.866			
Disposition to Privacy					**0.717**	**0.835**	**0.607**
DTP1	4.796	1.408	1.234	0.826			
DTP2	5.811	1.310	1.234	0.867			
DTP3	Deleted						
Privacy Concern					**0.865**	**0.950**	**0.922**
PC1	5.260	1.446	3.549	0.930			
PC2	5.267	1.499	3.723	0.934			
PC3	5.254	1.461	3.360	0.926			
Security Concern					**0.703**	**0.904**	**0.859**
SC1	4.292	1.648	1.864	0.776			
SC2	4.782	1.689	2.308	0.849			
SC3	4.553	1.635	2.675	0.870			
SC4	4.813	1.641	2.597	0.855			
Trust					**0.768**	**0.943**	**0.923**
T1	4.187	1.397	2.615	0.859			
T2	3.918	1.502	3.709	0.893			
T3	4.067	1.487	4.483	0.921			
T4	4.190	1.442	3.843	0.914			
T5	4.586	1.498	1.987	0.786			
Personal Interest					**0.787**	**0.917**	**0.865**
Interest1	4.355	1.582	2.290	0.886			
Interest2	4.384	1.515	2.196	0.880			
Interest3	4.337	1.611	2.425	0.895			
Perceived Usefulness					0.836	0.939	0.902
PU1	5.216	1.380	3.145	0.918			
PU2	4.867	1.435	2.577	0.896			
PU3	5.192	1.377	3.430	0.930			
Cloud Storage Reputation					**0.871**	**0.931**	**0.852**

(*continued on next page*)

Table 2 (*continued*)

Combined Sample N = 786							
First Order Constructs	Mean	SD	Outer VIF Values	Factor Loading	AVE	C.R.	Cronbach's Alpha
Rep1	Deleted						
Rep2	4.389	1.276	2.229	0.935			
Rep3	4.503	1.267	2.229	0.931			
Willingness to Put Less Sensitive Personal Information					**0.596**	**0.816**	**0.665**
Will1	4.720	1.747	1.170	0.760			
Will2	4.445	1.771	1.437	0.776			
Will3	3.590	1.865	1.443	0.780			
Willingness to Put More Sensitive Personal Information					**0.885**	**0.939**	**0.871**
Will4	2.414	1.720	2.475	0.950			
Will5	1.977	1.596	2.475	0.931			
Second Order Constructs (*Formative*)	**Mean**	**SD**		**Beta weight**	**AVE**	**C.R.**	**Cronbach's Alpha**
Perceived Cost					**0.498**	**0.916**	**0.898**
Privacy Concerns	5.260	1.469	–	0.367			
Privacy Risk	4.626	1.744	–	0.476			
Security Concerns	4.610	1.385	–	0.414			
Perceived Benefits					**0.621**	**0.908**	**0.878**
Personal Interest	4.359	1.569	–	0.541			
Perceived Usefulness	5.092	1.397	–	0.602			

50% (Harman, 1960). Second, a correlation matrix was examined for highly correlated factors (Bagozzi, Yi, & Phillips, 1991). CMV exists when there is an extremely high correlation ($r > 0.9$, other than square root of the AVE), yet the correlation analysis results found in the correlation table do not reveal such evidence. Based on these two indicators, we can conclude that our data is relatively robust against CMV.

5.3. PLS SEM path coefficient analysis results

We employed the PLS algorithm in SmartPLS 3.0 to generate the coefficient (β) value in our research framework. As mentioned, we used a repeated indicator approach to deal with the second order formative construct (for perceive cost and perceived benefit). The critical ratios to determine structural parameter significance were estimated via a bootstrapping procedure (Efron & Tibshirani, 1993). Hair et al. (2011) recommend using a bootstrap to assess the path coefficients' significance with a large number of re-sampling size such as 5000 number of bootstrap samples. Table 3 shows the PLS coefficient analysis results. Based on the combined sample results, we can conclude that hypotheses 10b and 11b are unsupported, while the rest of the hypotheses are supported. Fig. 2 depicts the results of the PLS SEM path coefficient analysis.

A structural parameter is significant (for the two-tails test) if it has a critical t-value higher than 1.96 (significance level = 5%), 2.58 (significance level = 1%), and 3.29 (significance level = 0.1%) (Hair et al., 2011).

5.4. Exploratory PLS SEM multi group analysis (PLS MGA)

We performed the PLS Multi Group Analysis (PLS MGA) using SmartPLS 3.0 to statistically confirm the significant difference of each specific path coefficient in relation to the two samples (Indonesia and Taiwan). This procedure applied the PLS MGA approach as suggested by Sarstedt, Henseler, and Ringle (2011) and Henseler, Ringle, and Sinkovics (2009). The bootstrapping procedure of 5000 re-sampling was performed to generate the results. A result is significant at the 5% probability of error level if the p-value is < 0.05 or p-value is > 0.95 for a specific difference in group-specific path coefficients. Table 4 reports the PLS MGA results.

Based on the PLS MGA results, it is evident that there are several significant differences in some paths. The two samples are significantly different with regard to the relationship between trust and willingness to put more sensitive personal information onto cloud storage (supporting Hypothesis 12c). The two samples are also significantly different with regard to the relationship between perceived effectiveness of government regulation and privacy control (supporting Hypothesis 12a).

6. Discussions

In general, the findings suggest that user willingness to put their personal information onto cloud storage is mainly affected by three dominant factors: perceived costs, perceived benefits, and trust. In line with CPMT, this study suggests cost-benefits cognitive assessment will play as a major role in determining user willingness, in which users tend to maximize benefits while reducing costs (Metzger, 2007; Petronio, 2002). With regard to less sensitive personal information, it can be seen from the results that the effect of perceived costs on user willingness is less significant as compared to the effect of perceived benefits on user willingness. On the other hand, for more sensitive personal information, the effect of perceived costs on user willingness is more significant as compared to the effect of perceived benefits on user willingness. Users might use cloud storage for different purposes, such as file backup, to carry data conveniently, or even to share information (Yang & Lin, 2015). It can be assumed that putting less sensitive

Table 3
PLS Coefficient Path Analysis for Combined Sample (cost-benefit second order formative).

H	Combined Sample Path	Coefficient	t-value	Collinearity Statistics (VIF)
Main Path				
1a	Trust– > Willingness to Put Less Sensitive Personal Information	0.184***	4.026	2.227
1b	Trust– > Willingness to Put More Sensitive Personal Information	0.153***	3.454	2.227
2a	Perceived Cost– > Willingness to Put Less Sensitive Personal Information	−0.072*	2.422	1.151
2b	Perceived Cost– > Willingness to Put More Sensitive Personal Information	−0.181***	4.955	1.151
3	Perceived Cost– > Trust	−0.152***	5.709	1.083
4a	Perceived Benefits– > Willingness to Put Less Sensitive Personal Information	0.472***	11.789	1.738
4b	Perceived Benefits– > Willingness to Put More Sensitive Personal Information	0.103**	2.638	1.738
5	Perceived Benefits– > Trust	0.483***	16.197	1.166
6	Privacy Control– > Trust	0.319***	10.100	1.237
7	Privacy Control– > Perceived Cost	−0.121**	2.690	1.755
8	Disposition to Privacy– > Perceived Cost	0.390***	11.104	1.069
9a	Perceived Effectiveness of Privacy Policy– > Privacy Control	0.209***	3.844	2.616
9b	Perceived Effectiveness of Privacy Policy– > Perceived Cost	−0.217***	4.369	2.896
10a	Perceived Effectiveness of Industry Self-Regulation– > Privacy Control	0.245***	4.608	3.027
10b	Perceived Effectiveness of Industry Self-Regulation– > Perceived Cost	−0.045	0.786	3.205
11a	Perceived Effectiveness of Government Regulation– > Privacy Control	0.275***	7.352	1.546
11b	Perceived Effectiveness of Government Regulation– > Perceived Cost	−0.069	1.656	1.741
Control Path				
	IT Background– > Willingness to Put Less Sensitive Personal Information	−0.030	1.053	1.034
	IT Background– > Willingness to Put More Sensitive Personal Information	−0.068*	2.005	1.034
	IT Background– > Perceived Cost	0.016	0.483	1.115
	Age– > Willingness to Put Less Sensitive Personal Information	0.027	0.920	1.183
	Age– > Willingness to Put More Sensitive Personal Information	0.061	1.574	1.183
	Age– > Perceived Cost	0.079*	2.223	1.243
	Gender– > Willingness to Put Less Sensitive Personal Information	−0.064	2.349	1.020
	Gender– > Willingness to Put More Sensitive Personal Information	−0.134***	4.285	1.020
	Gender– > Perceived Cost	0.044	1.479	1.029
	CSReputation– > Willingness to Put Less Sensitive Personal Information	0.025	0.628	1.764
	CSReputation– > Willingness to Put More Sensitive Personal Information	0.082*	2.099	1.764
	CSReputation– > Perceived Cost	−0.034	0.972	1.306
	Frequency using CS– > Perceived Cost	−0.026	0.719	1.308
	Education– > Willingness to Put Less Sensitive Personal Information	−0.054	1.792	1.147
	Education– > Willingness to Put More Sensitive Personal Information	−0.109**	2.898	1.147
	Education– > Perceived Cost	0.023	0.669	1.180

$^{*}p < 0.05$ $^{**}p < 0.01$ $^{***}p < 0.001$.

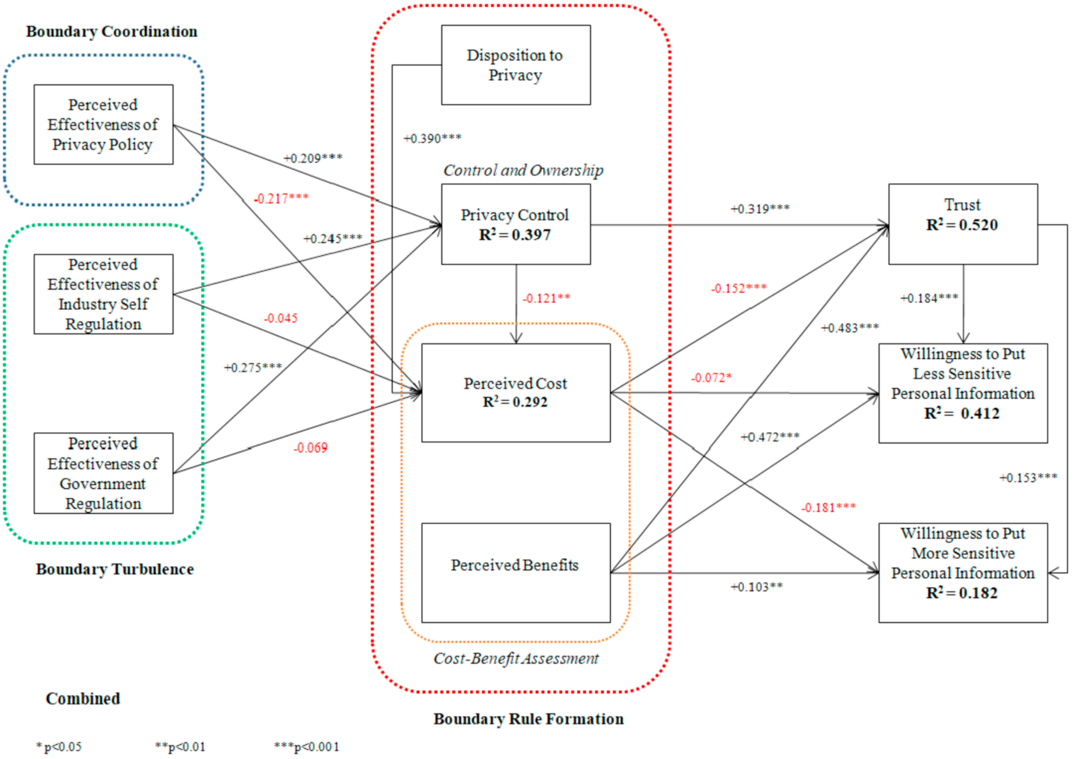

Fig. 2. PLS path analysis for combined sample.

Table 4
PLS MGA results.

Path	PLS-MGA	
	Path Coefficients Difference (Indonesia – Taiwan)	MGA p-value (Indonesia vs Taiwan)
Main Path		
Trust– > Willingness to Put Less Sensitive Personal Information	0.061	0.738
Trust– > Willingness to Put More Sensitive Personal Information	0.243 (Indonesia = 0.007, Taiwan = 0.250)	0.997*
Perceived Cost– > Willingness to Put Less Sensitive Personal Information	0.050	0.205
Perceived Cost– > Willingness to Put More Sensitive Personal Information	0.063	0.805
Perceived Cost– > Trust	0.039	0.754
Perceived Benefits– > Willingness to Put Less Sensitive Personal Information	0.126	0.948
Perceived Benefits– > Willingness to Put More Sensitive Personal Information	0.062	0.206
Perceived Benefits– > Trust	0.078	0.891
Privacy Control– > Trust	0.013	0.420
Privacy Control– > Perceived Cost	0.114	0.903
Disposition to Privacy– > Perceived Cost	0.101	0.924
Perceived Effectiveness of Privacy Policy– > Privacy Control	0.003	0.511
Perceived Effectiveness of Privacy Policy– > Perceived Cost	0.022	0.411
Perceived Effectiveness of Industry Self-Regulation– > Privacy Control	0.071	0.231
Perceived Effectiveness of Industry Self-Regulation– > Perceived Cost	0.022	0.418
Perceived Effectiveness of Government Regulation– > Privacy Control	0.289 (Indonesia = 0.123, Taiwan = 0.413)	1.000*
Perceived Effectiveness of Government Regulation– > Perceived Cost	0.036	0.658
Control Path		
IT Background– > Willingness to Put Less Sensitive Personal Information	0.043	0.767
IT Background– > Willingness to Put More Sensitive Personal Information	0.048	0.247
IT Background– > Perceived Cost	0.003	0.483
Age– > Willingness to Put Less Sensitive Personal Information	0.030	0.312
Age– > Willingness to Put More Sensitive Personal Information	0.041	0.712
Age– > Perceived Cost	0.147 (Indonesia = −0.023, Taiwan = 0.125)	0.974*
Gender– > Willingness to Put Less Sensitive Personal Information	0.099 (Indonesia = −0.005, Taiwan = −0.104	0.046*
Gender– > Willingness to Put More Sensitive Personal Information	0.069	0.145
Gender– > Perceived Cost	0.149 (Indonesia = −0.030, Taiwan = 0.120)	0.992*
CSReputation– > Willingness to Put Less Sensitive Personal Information	0.022	0.397
CSReputation– > Willingness to Put More Sensitive Personal Information	0.014	0.567
CSReputation– > Perceived Cost	0.086	0.132
Frequency using CS– > Perceived Cost	0.012	0.570
Education– > Willingness to Put Less Sensitive Personal Information	0.043	0.747
Education– > Willingness to Put More Sensitive Personal Information	0.224 (Indonesia = 0.001, Taiwan = −0.223)	0.001*
Education– > Perceived Cost	0.052	0.230

*p < 0.05 or p > 0.95.

personal information (e.g., work documents, music, videos, photos) onto cloud storage will be associated with more benefits related to such purposes.

Based on the PLS coefficient path analysis, we can conclude that Hypothesis 13a is supported. It thus seems reasonable to argue that, since the personal information is less sensitive, users might not feel any significant privacy or security threats when putting such personal information onto cloud storage. We may also assume that they even might not care very much if such personal information is sold by the cloud storage provider or stolen by hackers. On the contrary, more sensitive personal information (e.g., personal documents, personal identification, financial information, etc.) will tell a different story. Users will perceive significant threats related putting more sensitive personal information onto cloud storage, thus increasing perceived costs and reducing their willingness to put highly sensitive personal information on the cloud storage. With regard to the relationship with perceived benefit, although users might gain some benefits by putting such information onto storage, for example for backup purposes, perceived costs are still more prevalent than perceived benefits. This might imply that putting less sensitive personal information onto cloud storage may result in some perceived costs, however, putting more sensitive personal information on cloud storage will result in significantly greater perceived cost.

Considering different types of personal information will better explain why users are still willing to put personal information onto cloud storage. We might argue that high privacy and security concerns regarding cloud storage are more apparent in the case of more sensitive rather than less sensitive personal information. High concerns might only refer to more sensitive personal information, which can be translated to less willingness to put such information onto the cloud. Meanwhile, users are more willing to put less sensitive personal information there. This would explain why users are still willing to put their personal information onto storage in light of high privacy concerns since this “personal information” more likely is referring to less sensitive personal information instead of referring to more sensitive personal information. In addition, we also found that some control variables (IT background, age, cloud storage reputation, and education) have some effects on users' willingness to put more sensitive personal information. Nevertheless, regardless of the type of personal information, it is clear that in general users still have some privacy and security concerns for both types of information sensitivity.

Our results demonstrate the significant positive effect of trust on user willingness to put personal information onto cloud storage. In other words, when users have high trust in cloud storage providers, they will be more willing to put their personal information onto cloud storage. However, as mentioned in partially supported H13b, the effect of trust on users' willingness to put personal information onto cloud storage is stronger for more sensitive personal information than it is for less sensitive personal information (at least in Taiwan). This indicates the important role of trust in the use of cloud storage, in particular with regard to the user willingness within high UA cultures. This particular finding echoes the prior literature suggesting that trust in the cloud computing environment is very critical and should be built properly (King & Raja, 2012). Our finding further suggests that trust can be greatly increased through higher privacy control and lower perceptions of perceived cost. Meanwhile, perceived cost can be negatively affected by perceived effectiveness of privacy policy and privacy control and positively affected by disposition to privacy.

Privacy policies serve as a form of important institution-based trust as well as a signaling cue that is able to reduce perceived cost and increase privacy control. Because cloud storage deals with users' personal information directly, users might tend to critically examine the privacy policies of a cloud storage provider to ensure the overall privacy and security of the cloud storage environment. When users feel greater control over privacy, perceived cost will be reduced. Evidence from earlier studies indicated a strong negative effect of privacy policy on online privacy concerns (Wu et al., 2012).

Meanwhile, we found that disposition to privacy has a significant impact on perceived cost such as privacy concerns. This result is similar to the key findings of some previous studies e.g., (Li, 2014; Xu et al., 2011) that stressed the importance of privacy personality trait related construct in influencing privacy related costs. Furthermore, industry self-regulation and government regulation have a significant positive impact on privacy control. This implies that there is a significant role of third party institutional mechanisms in enhancing users' privacy control perceptions. However, as shown by the unsupported hypotheses (H10b and H11b), these two institutional mechanisms (industry and government regulation) are not powerful enough to mitigate perceived cost, which means stronger or more improved institutional mechanisms might be required. The improved institutional mechanisms are expected to result in a significant positive impact on privacy control and a significant negative impact on perceived cost.

According to the PLS MGA analysis results, we found that there are two path relationships that are considerably different in these two samples. We explained the differences by taking Hofstede (1991) two cultural dimensions (Uncertainty Avoidance and Long-term orientation) into consideration. The role of culture in this study is found to influence users' willingness to put personal information both directly and indirectly. Our findings therefore generally confirm the importance of culture in CPMT.

6.1. Theoretical implications

This study offers some important theoretical implications and contributions to academia. First, we extended and confirmed the application of CPMT in the IS domain. To the best of our knowledge, there are few IS-related studies that have applied CPMT as their main theoretical framework. In the current state of the IS literature, only a few previous studies have integrated CPMT within the IS context, e.g., (Metzger, 2007; Xu et al., 2011). Given the importance of CPMT in the privacy literature, this number is arguably still limited. Our study has extended Xu et al. (2011) research framework, which was guided by CPMT and institutional-based trust. Specifically, we applied their research framework within the context of cloud storage and further extended it by adding several important, relevant constructs. By doing this, we believe we have improved the explanatory power of CPMT within the context of our research in the area of cloud storage.

Second, we extended CPMT with the Privacy-Trust-Behavioral Intention Model. The findings indicate that trust is an important concept that should be taken into consideration when applying CPMT. Our proposed integrated model successfully explained why users are willing to put their personal information onto cloud storage. Because cloud storage is a new phenomenon in most IS literature, to date, only a few previous studies have empirically studied it e.g., (Menard et al., 2014; Yang & Lin, 2015). This study might be one of the earlier empirical studies aimed toward a better understanding cloud storage user behavior, particularly with regard to its end users' privacy, security, and privacy risk related issues.

Third, we also extended CPMT with the information sensitivity concept. Based on our best understanding of CPMT, the theory does not consider different types of information sensitivity in its theoretical formulation. In addition, most prior studies incorporating CPMT did not include the information sensitivity concept in their research model. This might lead to inaccurate results and interpretations, as they generalized the information sensitivity level of the personal information disclosed. Because different types of information sensitivity will be closely associated with individual privacy, by extending CPMT with the information sensitivity concept, this study might have contributed to the extension and improvement of CPMT.

Lastly, while CPMT emphasizes the importance of culture, it is surprising that there have been very limited prior studies that have applied CPMT with cultural differences. This study demonstrated that cultural differences influence two path relationships. We therefore contribute to the validity of CPMT by including cultural differences, particularly by taking the UA and PD cultural dimensions into account. Furthermore, we have provided some empirical evidence to the literature, such that CPMT can be successfully integrated (and extended) with Hofstede (1991) cultural dimension.

6.2. Practical implications

This study has several practical implications for cloud storage providers and governments. In light of our findings, cloud storage providers must make sure that they provide comprehensive privacy and security protection mechanisms to ensure the cloud storage users' personal information will always be kept safe and private. This is more critical for more sensitive personal information. Users might be worried that their sensitive personal information put onto cloud storage can be stolen, used without authorization, or improperly used by cloud storage providers, for example, being sold to profit-making organizations (Yang & Lin, 2015).

Although the findings might indicate that users are not concerned very much about perceived cost when putting less sensitive information on the cloud, protection is still absolutely required. As long as users still raise privacy and security concerns, it is likely that they do not trust cloud storage providers entirely. Thus, in order to enhance privacy and security protection, cloud storage providers should be focused on building user trust and should be trying to alleviate perceived cost as much as possible. Although challenging, trust building by ensuring privacy control, especially in Taiwan, is very important. Cloud storage providers focused on Taiwan should be aware that Taiwanese society is high in UA, in which they value certainty such as security and low-risk conditions. For this reason, privacy control has to be highly visible so that Taiwanese users can feel that they have full privacy control over the personal information they put onto cloud storage, thereby increasing their trust.

At the same time, cloud storage providers may also wish to provide more functions and better services to increase perceived benefits. For example, cloud storage providers could provide more drive space, customized functions, and possibly more advanced data compression techniques so that cloud storage users who have limited internet connections can still significantly benefit when placing or retrieving their personal information onto the cloud. This is vital especially for Indonesia because its Internet connection speed is much more limited as compared to Taiwan's. In terms of security protection, various encryption functions can be provided to ensure the safety of users' personal information. Excellent security and privacy protection mechanisms can be provided by cloud storage providers in order to avoid privacy risks (Wei et al., 2014). However, due to the high technicalities involved, users may not be aware of or believe that such mechanisms will be effective enough to increase their privacy control and reduce privacy costs. Here, institutional mechanisms might be able to facilitate trust.

We suggest that privacy policies should clearly mention how sensitive personal information is being handled and protected by cloud storage providers. Privacy policies can be enhanced to increase privacy control and therefore reduce perceived cost. To cater to cultural differences, privacy policies may be better customized or adjusted in accordance to each country's cultural characteristics. For example, in the case of a country with high UA, more detailed, stronger privacy policy statements could be provided. It might be possible that users have a limited understanding of these third party institutions, thus negatively influencing their effectiveness. Improved awareness and education related to industry self-regulation programs is also necessary to reduce perceived cost.

Both Indonesia and Taiwan have somewhat limited government regulations with regard to online personal data (Piper, 2013). Comprehensive laws that govern cloud computing-related issues should be promptly introduced. This is especially true for Taiwan as a country that has placed a lot of value on laws and regulations. Government enforcement should cover articles regarding sensitive personal information and how it will be kept private and secure in the cloud environment (King & Raja, 2012). The rules and regulations may not be effective to mitigate privacy costs if users are not even aware that such rules exist. After being legalized, such regulations then need to be made very public, especially to all cloud storage users in both countries.

6.3. Limitations and future research suggestions

As with many other previous studies, our study is not without limitations. We identify several key limitations of this study that future studies may further address. First, we employed a cross sectional survey in data collection. While earlier studies have used the same data collection method e.g., (Menard et al., 2014; Yang & Lin, 2015), it might not capture the actual cloud storage user behavior precisely. In addition, user behavior may change over time due to the dynamic nature of privacy-related issues (e.g., user perceptions maybe influenced by more current news or situations regarding cloud storage privacy and security breaches). Future studies therefore may further extend our study by adopting more objective measures in terms of data collection and possibly using a longitudinal approach.

Second, our sample characteristics with regard to age in both countries were not equal. Although age was included as a control variable, and its effect was not significant in some relationships, the quality of the sample might be improved if the sample from both countries was in a similar age range. This might be useful for cultural comparison. We employed convenience and snowballing data sampling techniques in both countries. Using this data collection method may generalize our sample in each country to some extent; however, our sample may not accurately represent the entire country's population. For that reason, when dealing with culture, random sampling may be better for future studies.

Third, we employed two of Hofstede's cultural dimensions to explain our results with regard to cultural differences between Indonesia and Taiwan. Following prior studies e.g., (Krasnova et al., 2012; Wu et al., 2012), we consider Hoftstede's theory as a national level construct in which the cultural scores for each country are already available. Thus, we did not consider the individual level cultural measures (e.g., applying Hofstede's framework at the individual level). Other than Hofstede, there is another cultural theory called National Identity also known as NATID proposed by Keilor et al. (1996) which may be able to further explain this study's results pertaining to cultural differences. Because there is a lot of a room for improvement, we invite future researchers to extend our study by employing individual level cultural variables and possibly other cultural theories to further enhance our understanding of culture-related variables in this specific topic.

Fourth, CPMT suggest that privacy maybe dependent on the context. In this study, we limit our investigation to the context of cloud storage for personal use. However, cloud storage can also be used specifically for businesses or organizations. In addition, there are other types of similar PCBAs that offer various functions such as finance, health, social media, etc. In light of CPMT, future studies can compare different contexts related to cloud computing services with regard to privacy and security related issues.

7. Conclusions

Drawing from CPMT and the Privacy-Trust-Behavioral Intention Model, we developed a research framework to empirically investigate users' willingness to put personal information onto cloud storage. We tested our research framework in both Indonesia and Taiwan. The findings suggest that trust, perceived cost, and perceived benefit are the main factors affecting users' willingness. We found that perceived cost is more apparent when users put more sensitive personal information than less sensitive personal information onto cloud storage. This strongly indicates that users' privacy and security concerns are actually being addressed in regard to sensitive personal information only. Meanwhile, since perceived benefit is far greater than perceived cost, users may not be concerned that much when putting less sensitive personal information onto cloud storage.

Institutional privacy assurances such as privacy policies, industry self-regulation, and government regulations seem to work relatively well in terms of positively influencing privacy control. However, industry self-regulation and government regulation might not be so effective with regard to reducing perceived cost. This might because government regulations pertaining to cloud computing are still in their infancy, especially in the case of local government regulations in these countries. Because more users have put their personal information on the cloud, strong regulations are urgently needed. Drawing from Hofstede's culture theory, this study successfully identified that culture also plays an important part in influencing users' perceptions regarding privacy, particularly within the context of cloud storage.

Appendix A. Measurement Items

		Initial or Original Items from the Source	Source or Adaptation
Perceived Effectiveness of Privacy Policy			
	Privacy Policy refers to the statements prescribed by Cloud Storage provider with regard to its privacy and security practices.		
PEPP1	I feel confident that Cloud Storage Provider's privacy statements reflect their commitments to protect my personal information that I put onto cloud storage.	*I feel confident that these websites' privacy statements reflect their commitments to protect my personal information.*	(Xu et al., 2011)
PEPP2	With the privacy statements, I believe the personal information that I put onto cloud storage will be kept personal and confidential by the provider.	*With their privacy statements, I believe that my personal information will be kept private and confidential by these websites.*	
PEPP3	I believe that the cloud storage provider's privacy statements are an effective way to demonstrate the provider's commitments to privacy.	*I believe that these websites' privacy statements are an effective way to demonstrate their commitments to privacy.*	
Perceived Effectiveness of Industry Self-Regulation			
	Industry Self-Regulation refers to the third party institutions such as TRUSTe, Cloud Security Alliance or other similar privacy approval programs to independently assure users' privacy on the Cloud.		
PEISR1	I believe that privacy seal of approval programs will impose sanctions for cloud storage provider non-compliance with privacy policies.	*I believe that privacy seal of approval programs such as TRUSTe will impose sanctions for online companies' noncompliance with its privacy policy.*	(Xu et al., 2011)
PEISR2	A privacy seal of approval program will stand by me if my personal information place onto cloud storage is misused.	*Privacy seal of approval programs such as TRUSTe will stand by me if my personal information is misused during and after transactions with online companies.*	
PEISR3	I am confident that the privacy seal of approval program is able to address violations of my personal information place onto cloud storage.	*I am confident that privacy seal of approval programs such as TRUSTe is able to address violation of the information I provided to online companies.*	
Perceived Effectiveness of Government Regulation			
	Government regulations which are related to online personal data.		
PEGRL1	I believe that the Taiwan/Indonesia government will impose sanctions for cloud storage provider non-compliance with privacy policies.	*I believe that privacy seal of approval programs such as TRUSTe will impose sanctions for online companies' noncompliance with its privacy policy.*	(Xu et al., 2011) Adapted and Modified to the Government Context
PEGRL2	The Taiwan/Indonesia government will stand by me if my personal information placed onto cloud storage is misused.	*Privacy seal of approval programs such as TRUSTe will stand by me if my personal information is misused during and after transactions with online companies.*	
PEGRL3	I am confident that the Taiwan/Indonesia government is able to address violations of my personal information place onto cloud storage.	*I am confident that privacy seal of approval programs such as TRUSTe is able to address violation of the information I provided to online companies.*	
Privacy Control			
C1	I believe I have control over who can gain access to my personal information that I put on cloud storage.	*I believe I have control over who can get access to my personal information collected by this website.*	(Xu et al., 2011)
C2	I think I have control over the personal information that I put onto cloud storage that is released by the provider.	*I think I have control over what personal information is released by this website.*	
C3	I believe I have control over how my personal information that I put onto Cloud Storage is used by the provider.	*I believe I have control over how personal information is used by this website.*	
C4	I do not believe I can control my personal information that I put onto cloud storage. (R)	*I believe I can control my personal information provided to this website.*	
Privacy Risk			
	What do you believe is the risk for Cloud Storage users due to the possibility that:		
R1	My personal information that I put on cloud storage could be sold to third parties.	*Records of transactions could be sold to third parties?*	(Dinev & Hart, 2006)
R2	My personal information that I put on cloud storage could be misused.	*Personal information submitted could be misused?*	
R3	My personal information that I put on cloud storage could be made available to unknown individuals or companies without my knowledge.	*Personal information could be made available to unknown individuals or companies without your knowledge?*	
R4	My personal information that I put on cloud storage could be made available to government agencies.	*Personal information could be made available to government agencies?*	

Disposition to Privacy			
DTP1	Compared to others, I am more sensitive about the way companies handle my personal information.	*Compared to others, I am more sensitive about the way companies handle my personal information.*	(Xu et al., 2011)
DTP2	To me, it is the most important thing to keep my information privacy.	*To me, it is the most important thing to keep my information privacy.*	
DTP3	Compared to others, I tend not to be more concerned about threats to my information privacy. (R)	*Compared to others, I tend to be more concerned about threats to my information privacy.*	
Privacy Concern			
PC1	I am concerned that my personal information I put onto cloud storage could be misused.	*I am concerned that the information I submit on the Internet could be misused.*	(Dinev & Hart, 2006)
PC2	I am concerned that a person can find my personal information that I put onto cloud storage.	*I am concerned that a person can find private information about me on the Internet.*	
PC3	I am concerned about putting my personal information onto cloud storage because of what others might do with it.	*I am concerned about submitting information on the Internet, because of what others might do with it.*	
Security Concern			
SC1	I would not feel secure putting my personal information onto cloud storage.	*I would feel secure sending sensitive information across the World Wide Web.*	(Nepomuceno et al., 2014)
SC2	I would not feel totally safe putting my personal information onto cloud storage.	*I would feel totally safe providing sensitive information about myself over the World Wide Web.*	
SC3	Cloud storage is not a secure place to put my personal information.	*The World Wide Web is a secure means through which to send sensitive information.*	
SC4	Overall, cloud storage is not a safe place to put my personal information.	*Overall, the World Wide Web is a safe place to transmit sensitive information.*	
Trust			
T1	Cloud storage providers are trustworthy.	*This store is trustworthy.*	(Doney & Cannon, 1997; Jarvenpaa, Tractinsky, & Vitale, 2000) Adapted and Modified
T2	Cloud storage providers have my best interest in mind.	*I trust this store keeps my best interest in mind.*	
T3	Cloud storage providers will keep their promises made to me.	-	
T4	I believe the information that cloud storage providers provide me.	*I believe in the information that this vendor provides me*	
T5	Cloud storage providers want to be known as those who keep promises and commitments.	*This store wants to be known as one who keeps promises and commitments.*	
Personal Interest			
Interest1	I find that my interest in obtaining and using the personal information I put onto cloud storage overrides my concerns related to possible risk or vulnerability I may have regarding my privacy.	*I find that personal interest in the information that I want to obtain from the Internet overrides my concerns of possible risk or vulnerability that I may have regarding my privacy.*	(Dinev & Hart, 2006)
Interest2	The greater my interest in obtaining and using my personal information in cloud storage, the more I tend to suppress my privacy concerns.	*The greater my interest to obtain a certain information or service from the Internet, the more I tend to suppress my privacy concerns.*	
Interest3	In general, my need to obtain and use my personal information in cloud storage is greater than my concern about privacy.	*In general, my need to obtain certain information or services from the Internet is greater than my concern about privacy.*	
Perceived Usefulness			
PU1	Cloud storage is benefits me.	*The WWW is of benefit to me.*	(Limayen, Hirt, & Cheung, 2007)
PU2	The advantages of cloud storage outweigh the disadvantages.	*The advantages of the WWW outweigh the disadvantages.*	
PU3	Overall, using cloud storage is advantageous.	*Overall, using the WWW is advantageous.*	
Cloud Storage Reputation			
Rep1	Cloud storage providers have a bad reputation. (R)	*The vendor of this site has a good reputation.*	(Hsu, Chuang, & Hsu, 2014)
Rep2	Cloud storage providers are known to be concerned about customers.	*The vendor of this site is known to be concerned about customers.*	
Rep3	Cloud storage provider have a reputation for being honest.	*The vendor of this site has a reputation for being honest.*	

Willingness to Put Personal Information onto Cloud Storage

Please indicate your willingness level to put the following personal information type onto *Cloud Storage* (e.g. *Google Drive, Drop Box, One Drive, etc.):*

Will1	Your work related documents (e.g. for school, work, business).	*Purchase goods (e.g., books or CDs) or services (e.g., airline tickets or hotel reservations) from websites that require me to submit accurate and identifiable information (i.e. credit card information).*	(Dinev & Hart, 2006), (Forrester, 2012) Adapted and Modified
Will2	Your personal media (e.g. photos, videos, and music).	*Retrieve information from websites that require me to submit accurate and identifiable registration information, possibly including credit card information (e.g., using sites that provide personalized stock quotes, insurance rates, or loan rates; or using sexual or gambling websites).*	
Will3	Your personal documents (e.g. agendas, diary, notes, etc.)	*Conduct sales transactions at e-commerce sites that require me to provide credit card information (e.g., using sites for purchasing goods or software).*	
Will4	Your personal identity information (e.g. passport, national ID, phone, address, etc.).	*Retrieve highly personal and a password-protected financial information (e.g., using websites that allow me to access my bank account or my credit card account)*	
Will5	Your specific sensitive information (e.g. banking, credit card, health records, etc.)	–	

Appendix B. Descriptive statistics and PLS-CFA results for sub-sample (Second Order Formative)

First Order Constructs	Indonesia Sample N = 383							Taiwan Sample N = 403						
	Mean	SD	Outer VIF Values	Factor Loading	AVE	C.R.	Cronbach's Alpha	Mean	SD	Outer VIF Values	Factor Loading	AVE	C.R.	Cronbach's Alfa
Perceived Effectiveness of Privacy Policy					**0.763**	**0.906**	**0.846**					**0.864**	**0.950**	**0.921**
PEPP1	4.859	1.324	1.918	0.844				3.421	1.509	3.008	0.916			
PEPP2	4.613	1.414	2.127	0.901				3.531	1.564	4.074	0.944			
PEPP3	5.117	1.350	2.076	0.874				3.488	1.612	3.509	0.929			
Perceived Effectiveness of Industry Self-Regulation					**0.814**	**0.929**	**0.886**					**0.819**	**0.931**	**0.889**
PEISR1	4.778	1.380	2.364	0.890				3.536	1.625	2.149	0.854			
PEISR2	4.736	1.322	2.935	0.911				3.697	1.589	3.546	0.937			
PEISR3	4.467	1.356	2.475	0.904				3.464	1.535	2.987	0.921			
Perceived Effectiveness of Government Regulation					**0.882**	**0.957**	**0.933**					**0.813**	**0.929**	**0.884**
PEGRL1	3.757	1.715	3.302	0.921				3.590	1.643	2.170	0.861			
PEGRL2	3.584	1.686	4.806	0.953				3.295	1.583	4.953	0.953			
PEGRL3	3.454	1.655	4.215	0.943				3.091	1.623	3.469	0.889			
Privacy Control					**0.762**	**0.906**	**0.844**					**0.857**	**0.947**	**0.917**
C1	4.616	1.565	1.826	0.848				3.995	1.661	2.747	0.909			
C2	4.151	1.542	2.092	0.875				4.099	1.692	3.840	0.936			
C3	4.177	1.561	2.265	0.896				4.069	1.640	3.603	0.932			
C4	Deleted									Deleted				
Privacy Risk					**0.814**	**0.946**	**0.923**					**0.819**	**0.948**	**0.926**
R1	4.219	1.871	3.224	0.893				4.612	1.661	3.341	0.900			
R2	4.582	1.834	4.766	0.934				4.838	1.556	4.157	0.922			
R3	4.404	1.891	4.129	0.924				4.826	1.611	4.063	0.922			
R4	4.629	1.830	2.581	0.855				4.863	1.629	2.773	0.876			
Disposition to Privacy					**0.723**	**0.839**	**0.618**					**0.711**	**0.831**	**0.600**
DTP1	4.848	1.402	1.250	0.835				4.746	1.414	1.224	0.800			
DTP2	6.020	1.186	1.250	0.865				5.612	1.390	1.224	0.885			
DTP3	Deleted									Deleted				
Privacy Concern					**0.910**	**0.968**	**0.950**					**0.815**	**0.930**	**0.886**

PC1	5.114	1.554	3.918	0.935				5.379	1.326	3.303	0.923			
PC2	5.159	1.542	6.961	0.962				5.369	1.452	2.774	0.902			
PC3	5.154	1.496	7.112	0.964				5.349	1.422	2.347	0.882			
Security Concern					**0.755**	**0.925**	**0.892**					**0.650**	**0.880**	**0.820**
SC1	4.227	1.615	2.767	0.878				4.354	1.678	1.568	0.665			
SC2	4.524	1.668	2.815	0.871				5.027	1.675	1.983	0.809			
SC3	4.073	1.593	2.797	0.871				5.001	1.543	2.776	0.876			
SC4	4.517	1.635	2.560	0.855				5.094	1.599	2.608	0.858			
Trust					**0.704**	**0.921**	**0.891**					**0.793**	**0.950**	**0.934**
T1	4.595	1.206	2.432	0.861				3.799	1.456	2.600	0.847			
T2	4.174	1.337	3.131	0.876				3.674	1.608	4.024	0.902			
T3	4.302	1.297	3.577	0.901				3.784	1.618	5.234	0.934			
T4	4.430	1.246	3.021	0.890				3.962	1.574	4.501	0.927			
T5	5.054	1.193	1.389	0.637				4.141	1.619	2.582	0.839			
Personal Interest					**0.793**	**0.920**	**0.870**					**0.780**	**0.914**	**0.859**
Interest1	4.454	1.458	2.450	0.897				4.260	1.688	2.242	0.879			
Interest2	4.535	1.387	2.289	0.881				4.240	1.615	2.190	0.877			
Interest3	4.564	1.467	2.462	0.894				4.121	1.712	2.367	0.894			
Perceived Usefulness					**0.796**	**0.921**	**0.871**					**0.850**	**0.945**	**0.912**
PU1	5.644	1.177	3.198	0.915				4.808	1.435	2.882	0.911			
PU2	5.135	1.311	1.831	0.836				4.612	1.502	3.492	0.927			
PU3	5.603	1.152	3.253	0.922				4.801	1.459	3.380	0.927			
Cloud Storage Reputation					**0.860**	**0.925**	**0.838**					**0.877**	**0.935**	**0.861**
Rep1	Deleted									Deleted				
Rep2	4.470	1.157	2.088	0.913				4.312	1.377	2.328	0.945			
Rep3	4.561	1.137	2.088	0.941				4.449	1.378	2.328	0.928			
Willingness to Put Less Sensitive Personal Information					**0.520**	**0.764**	**0.553**					**0.699**	**0.874**	**0.784**
Will1	5.208	1.530	1.077	0.753				4.255	1.815	1.471	0.793			
Will2	4.378	1.830	1.244	0.687				4.508	1.712	1.756	0.848			
Will3	3.292	1.847	1.280	0.720				3.873	1.841	1.806	0.865			
Willingness to Put More Sensitive Personal Information					**0.845**	**0.916**	**0.818**					**0.933**	**0.965**	**0.928**
Will4	2.535	1.729	1.921	0.935				2.300	1.705	3.997	0.970			
Will5	1.809	1.396	1.921	0.904				2.136	1.753	3.997	0.961			
Second Order Constructs (*Formative*)	Mean	SD		Beta weight	AVE	C.R.	Cronbach's Alpha	Mean	SD		Beta Weight	AVE	C.R.	Cronbach's Alpha
Perceived Cost					**0.483**	**0.911**	**0.893**					**0.511**	**0.918**	**0.902**
Privacy Concerns	5.142	1.531	–	0.369				5.366	1.400	–	0.363			
Privacy Risk	4.459	1.857	–	0.420				4.785	1.614	–	0.508			
Security Concerns	4.335	1.414	–	0.505				4.871	1.307	–	0.341			
Perceived Benefits					**0.582**	**0.893**	**0.856**					**0.638**	**0.913**	**0.886**
Personal Interest	4.518	1.437	–	0.572				4.207	1.672	–	0.531			
Perceived Usefulness	5.461	1.213	–	0.595				4.740	1.465	–	0.599			

Appendix C. Correlation Table

		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1	Age	1000																		
2	CS Reputation	0.097	**0.933***																	
3	Disposition to Privacy	0.112	0.080	**0.847***																
4	Education	0.316	−0.002	0.046	1000															
5	FreqUsingCS	−0.105	0.156	0.142	0.148	1000														
6	Gender	−0.118	−0.053	−0.052	−0.067	0.024	1000													
7	IT Background	0.028	0.004	0.093	0.153	0.237	−0.009	1000												
8	PEGR	−0.047	0.342	0.091	−0.063	0.131	−0.003	0.086	**0.921***											
9	PEISR	−0.134	0.354	0.169	−0.021	0.365	−0.042	0.160	0.592	**0.916***										
10	PEPP	−0.161	0.381	0.138	−0.015	0.384	−0.063	0.192	0.498	0.785	**0.922***									
11	Perceived Usefulness	0.028	0.471	0.147	0.082	0.428	−0.044	0.120	0.250	0.418	0.476	**0.915***								
12	Personal Interest	0.032	0.429	0.031	0.037	0.188	−0.029	0.043	0.294	0.272	0.318	0.530	**0.887***							
13	Privacy Concern	0.148	−0.105	0.377	0.044	−0.075	0.042	0.071	−0.110	−0.115	−0.161	−0.084	−0.091	**0.930***						
14	Privacy Control	−0.129	0.381	0.145	−0.054	0.250	−0.003	0.028	0.524	0.572	0.538	0.369	0.284	−0.132	**0.900***					
15	Privacy Risk	0.132	−0.120	0.233	0.073	−0.050	−0.016	−0.031	−0.257	−0.276	−0.279	−0.078	−0.058	0.425	−0.277	**0.904***				
16	Security Concern	0.163	−0.177	0.199	0.063	−0.152	0.054	−0.042	−0.210	−0.282	−0.339	−0.118	−0.152	0.499	−0.224	0.419	**0.838***			
17	Trust	−0.017	0.628	0.091	0.006	0.267	−0.048	0.047	0.470	0.539	0.607	0.575	0.513	−0.187	0.542	−0.242	−0.290	**0.876***		
18	Less Sensitive Personal Information	0.019	0.402	0.037	−0.017	0.263	−0.095	0.018	0.255	0.287	0.367	0.569	0.487	−0.164	0.313	−0.134	−0.178	0.517	**0.772***	
19	More Sensitive Personal Information	0.016	0.275	−0.114	−0.097	−0.040	−0.155	−0.063	0.284	0.088	0.169	0.148	0.315	−0.241	0.133	−0.189	−0.185	0.325	0.457	**0.941***

*Square root of AVE.

References

Alsmadi, D., & Prybutok, V. (2018). Sharing and storage behavior via cloud computing: Security and privacy in research and practice. *Computers in Human Behavior, 85*, 218–226.

Arpaci, I. (2016). Understanding and predicting students' intention to use mobile cloud storage services. *Computers in Human Behavior, 58*, 150–157.

Bagozzi, R., Yi, Y., & Phillips, L. (1991). Assessing construct validity in organizational research. *Administrative Science Quarterly, 36*(3), 421–458.

Bansal, G., Zahedi, F., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems, 49*(2), 138–150.

Bansal, G., Zahedi, F. M., & Gefen, D. (2015). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management*. https://doi.org/10.1016/j.im.2015.08.001.

Barker, I. (2015). Cloud storage survey highlights governance and security concerns. [Electronic Version]. Retrieved August 19, 2018, from https://betanews.com/2015/06/02/cloud-storage-survey-highlights-governance-and-security-concerns/.

Bellman, S., Johnson, E. J., & Kobrin, S. J. (2004). International differences in information privacy concerns: A global survey of consumers. *The Information Society: International Journal, 20*(5), 313–324.

Cao, J., & Everard, A. (2008). User attitude towards instant messaging: The effect of espoused national cultural values on awareness and privacy. *Journal of Global Information Technology Management, 11*(2), 27–45.

Child, J., Haridakis, P. M., & Petronio, S. S. (2012). Blogging privacy rule orientations, privacy management, and content deletion practices: The variability of online privacy management activity at different stages of social media use. *Computers in Human Behavior, 28*(5), 1859–1872.

Chin, W. W. (1998a). Issues and opinions on structural equation modeling. *MIS Quarterly, 22*(1), 7–10.

Chin, W. W. (1998b). The partial least squares approach to structural equation modelling. In G. A. Marcoulides (Ed.). *Modern methods for business research*. Mahwah, New Jersey, United States of America: Lawrence Erlbaum.

Chiou, A. Y., Chen, J.-C., & Bisset, C. (2007). Cross cultural perceptions on privacy in the United States, Vietnam, Indonesia, and Taiwan. In K. Chen, & A. Fadlalla (Eds.). *Online consumer protection: Theories of human relativism*. Hershey, PA: Idea Group.

Chou, T.-S. (2013). Security threats on cloud computing vulnerabilities. *International Journal of Computer Science and Information Technology, 5*(3), 79–88.

Chu, C.-K., Zhu, W.-T., Han, J., Liu, J. K., Xu, J., & Zhou, J. (2013). Security concerns in popular cloud storage services. *Pervasive Computing, 12*(4), 50–57.

Cockcroft, S., & Rekker, S. (2015). The relationship between culture and information privacy policy. *Electronic Markets*. https://doi.org/10.1007/s12525-015-0195-9.

Cranor, L. F., Reagle, J., & Ackerman, M. S. (1999). *Beyond concern: Understanding net users attitudes about online privacy* AT&T Labs-Research Technical Report TR 99.4.3.

Culnan, M. J., & Amstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science, 10*(1), 104–115.

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues, 59*(2), 323–342.

D'Souza, & Phelps, J. E. (2009). The privacy paradox: The case of secondary disclosure. *Review of Marketing Science, 7*(4), 1–29.

Dinev, T., & Hart, P. (2004). Internet privacy concern and their antecedents - measurement validity and a regression model. *Behaviour & Information Technology, 23*(6), 413–422.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61–80.

Doney, P. M., & Cannon, J. P. (1997). An examination of the nature of trust in buyer-seller relationships. *Journal of Marketing, 61*(2), 35–51.

Du, M., Wang, Q., & He, M. (2018). Privacy-preserving indexing and query processing for secure dynamic cloud storage. *IEEE Transactions on Information Forensics and Security, 13*(9), 2320–2332.

Efron, B., & Tibshirani, R. J. (1993). *An introduction to the bootstrap*. New York, United States of America: Chapman and Hall.

Fornell, C., & Larcker, D. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(3), 39–50.

Forrester (2012). *Personal cloud services emerge to orchestrate our mobile computing lives*. Cambridge, MA: Forrester Research, Inc (Forrester).

Gasiorowski-Denis, E. (2015). Trust and confidence in cloud privacy. [Electronic Version]. Retrieved August 19, 2018, from https://www.iso.org/news/2015/01/Ref1921.html.

Gefen, D., Karahanna, E., & Straub, D. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly, 27*(1), 51–90.

Ghaffari, K., & Lagzian, M. (2018). Exploring users' experiences of using personal cloud storage services: A phenomenological study. *Behaviour & Information Technology, 37*(3), 295–309.

Gibbons, F. X., & Gerrard, M. (1995). Predicting young adults' health risk behavior. *Journal of Personality and Social Psychology, 69*(3), 505–517.

Hair, J. F., Ringle, C. M., & Marko, S. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice, 19*(2), 139–151.

Harman, H. H. (1960). *Modern factor analysis*. Chicago, IL: University of Chicago Press.

Henseler, J., Ringle, C. M., & Sinkovics, R. R. (2009). The use of partial least square modelling in international marketing. *Advances in International Marketing, 20*(0), 277–320.

Hew, K. F. (2011). Students' teachers' use of facebook. *Computers in Human Behavior, 27*(2), 662–676.

Hofstede, G. (1991). *Culture and organizations: Software of the mind*. London: McGraw-Hill.

Hofstede, G. (2001). *Culture's consequences: Comparing values, behaviors, institutions, and organizations accross nations*. Thousand Oaks, CA: Sage.

Hofstede, G. (2011). Dimensionalizing cultures: The hofstede model in context. *Online Readings in Psychology and Culture, 2*(1)https://doi.org/10.9707/2307-0919.1014.

Hsu, M.-H., Chuang, L.-W., & Hsu, C.-S. (2014). Understanding online shopping intention: The roles of four types of trust and their antecedents. *Internet Research, 24*(3), 332–352.

Hui, K. L., Teo, H.-H., & Lee, S. Y. T. (2007). The value of privacy assurance: An exploratory field experiment. *MIS Quarterly, 31*(1), 19–33.

Jarvenpaa, S. L., Tractinsky, N., & Vitale, M. (2000). Consumer trust in an internet store. *Information Technology and Management, 1*(1–2), 45–71.

Jiang, Z. J., Heng, C. S., & Choi, B. C. F. (2013). Privacy concerns and privacy-protective in synchronous online social interactions. *Information Systems Research, 24*(3), 579–595.

Johnson, E. M. (2018). Thousands of FedEx customer records exposed by unsecured server. [Electronic Version]. Retrieved August 19, 2018, from https://www.businessinsider.com/r-thousands-of-fedex-customer-records-exposed-by-unsecured-server-2018-2/?IR=T.

Kalloniatis, C., Mouratidis, H., Vassilis, M., Islam, S., Gritzalis, S., & Kavakli, E. (2014). Towards the design of secure and privacy-oriented information systems in the cloud: Identifying the major concepts. *Computer Standards & Interfaces, 36*(4), 759–775.

Keillor, B. D., Hult, G. T. M., Erffmeyer, R. C., & Babakus, E. (1996). NATID: The development and application of a national identity measure for use in international marketing. *Journal of International Marketing, 4*(2), 57–73.

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human-computer Studies, 71*(12), 1163–1173.

King, N. J., & Raja, V. T. (2012). Protecting privacy and security of sensitive customer data in the cloud. *Computer Law & Security Review, 28*(3), 308–319.

Kohgadai, A. (2018). 9 stats IT should know on sensitive data stored and shared in the cloud. [Electronic Version]. Retrieved August 19, 2018, from https://www.skyhighnetworks.com/cloud-security-blog/9-stats-it-should-know-on-sensitive-data-stored-and-shared-in-the-cloud/.

Krasnova, H., Veltri, N. F., & Günther, O. (2012). Self-disclosure and privacy calculus on social networking sites: The role of culture. *Business and Information Systems Engineering, 4*(3), 127–135.

Leidner, D., & Kayworth, T. (2006). A review of culture in information systems research: Toward a theory of information technology culture conflict. *Management Information Systems Quarterly, 30*(2), 357–399.

Lewis, D. (2014). iCloud data breach: Hacking and celebrity photos. [Electronic Version]. Retrieved August 19, 2018, from https://www.forbes.com/sites/davelewis/2014/09/02/icloud-data-breach-hacking-and-nude-celebrity-photos/#341da9602de7.

Li, Y. (2014). The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. *Decision Support Systems, 57*(00), 343–354.

Li, Y., Chang, K.-C., & Wang, J. (2017). Self-determination and perceived information control in cloud storage service. *Journal of Computer Information Systems,* 1–11. https://doi.org/10.1080/08874417.2017.1405294.

Limayen, M., Hirt, S. G., & Cheung, C. M. K. (2007). How habit limits the predictive power of intention: The case of information systems continuance. *MIS Quarterly, 31*(4), 705–737.

Liu, C., Marchewka, J. T., Lu, J., & Yu, C.-S. (2005). Beyond concern - a privacy-trust-behavioral intention model of electronic commerce. *Information & Management, 42*(2), 289–304.

Lowry, P. B., Cao, J., & Everard, A. (2011). Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *Journal of Management Information Systems, 27*(4), 163–200.

Lowry, P. B., & Gaskin, J. (2014). Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: When to choose it and how to use it. *IEEE Transactions on Professional Communication, 57*(2), 123–146.

Malhotra, N. K., & Dash, S. (2011). *Marketing research: An applied orientation*. New Delhi: Pearson Inc.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research, 13*(3), 334–359.

Menard, P., Gatlin, R., & Warkentin, M. (2014). Threat protection and convenience: Antecedents of cloud-based data backup. *Journal of Computer Information Systems, 55*(1), 83–91.

Metzger, M. J. (2007). Communication privacy management in electronic commerce. *Journal of Computer-mediated Communication, 12*(2), 335–361.

Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing, 18*(3), 15–29.

Nepomuceno, M. V., Laroche, M., & Richard, M.-O. (2014). 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), 619–629.

Ng, C. S.-P. (2013). Intention to purchase on social commerce websites accross cultures: A cross-regional study. *Information & Management, 50*, 609–620.

Nowak, G. J., & Phelps, J. (1997). Direct marketing and the use of individual-level consumer information: Determining how and when 'privacy' matters. *Journal of Direct Marketing, 11*(4), 94–108.

Nunally, J. C. (1978). *Psychometric theory*. New York, United States of America: McGraw-Hill.

Petronio, S. S. (2002). *Boundaries of privacy: Dialectics of disclosure.* Albany, NY: State University of New York Press.

Petronio, S. (2013). Brief status report on communication privacy management theory. *Journal of Family Communication, 13*(1), 6–14.

Petronio, S., & Durham, W. T. (2008). Communication privacy management theory: Significance for interpersonal communication. In L. A. Baxter, & D. O. Braithwaite (Eds.). *Engaging theories in interpersonal communication multiple perspectives* (pp. 309–322). Thousand Oaks, CA: SAGE Publications, Inc.

Piper, D. (2013). Data protection laws of the world. USA: DLA piper. Retrieved July 11, 2015 from https://files.dlapiper.com/files/Uploads/Documents/Data_Protection_Laws_of_the_World_2013.pdf.

Podsakoff, P. M., Mackenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*(5), 839–903.

Raykov, T. (2001). On the use and utility of the reliability coefficient in social and behavioral research. *Quality and Quantity, 35*(3), 253–263.

Ringle, C. M., Sven, W., & Jan-Michael, B. (2015). *SmartPLS. Bönningstedt: SmartPLS*.

Sarstedt, M., Henseler, J., & Ringle, C. M. (2011). Multi-group analysis in partial least squares (PLS) path modelling: Alternative methods and empirical results. *Advances in International Marketing, 22*(1), 195–218.

Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of Public Policy and Marketing, 19*(1), 62–63.

Slyke, C. V., Shim, J. T., Johnson, R., & Jiang, J. (2006). Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems, 7*(6), 415–444.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989–1015.

Statista (2018). Forecast number of personal cloud storage consumers/users worldwide from 2014 to 2020 (in millions). [Electronic Version]. Retrieved August 19, 2018, from https://www.statista.com/statistics/499558/worldwide-personal-cloud-storage-users/.

Ward, S., Bridges, K., & Chitty, B. (2005). Do incentives matter? An examination of online privacy concerns and willingness to provide personal and financial information. *Journal of Marketing Communications, 11*(1), 21–40.

Weible, R. J. (1993). *Privacy and data: An empirical study of the influence and types and data and situational context upon privacy perceptions in department of business administration.* Mississippi State University.

Wei, L., Zhu, H., Cao, Z., Dong, X., Jia, W., & Chen, Y. (2014). Security and privacy for storage and computation in cloud computing. *Information Sciences, 258*(2014), 371–386.

Wilson, B. (2010). Using PLS to investigate interaction effects between higher order branding constructs. In V. Esposito Vinzi, W. W. Chin, J. Henseler, & H. Wang (Eds.). *Handbook of partial least squares, concepts, methods, and applications*. Berlin, Heidelberg: Springer Handbooks.

Wu, L., Chen, B., Zeadally, S., & He, D. (2018). An efficient and secure searchable public key encryption scheme with privacy protection for cloud storage. *Soft Computing,* 1–12.

Wu, K.-W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior, 28*(3), 889–897.

Wu, K., Vassileva, J., & Zhao, Y. (2017). Understanding users' intention to switch personal cloud storage services: Evidence from the Chinese market. *Computers in Human Behavior, 68*, 300–314.

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems, 12*(12), 798.

Xu, H., Teo, H.-H., Tan, B. C. Y., & Agarwal, R. (2009). The role of push-pull technology in privacy calculus: The case of location-based services. *Journal of Management Information Systems, 26*(3), 135–173.

Xu, H., Teo, H.-H., Tan, B. C. Y., & Agarwal, R. (2010). The role of push-pull technology in privacy calculus: The case of location based service. *Journal of Management Information Systems, 26*(3), 135–174.

Yang, H.-L., & Lin, S.-L. (2015). User continuance intention to use cloud storage service. *Computers in Human Behavior, 52*(2015), 219–232.

Yang, S., & Wang, K. (2009). The influence of information sensitivity compensation on privacy concern and behavioral intention. *The Data Base for Advances in Information Systems, 40*(1), 38–51.

Yoon, C. (2009). The effects of national culture values on consumer acceptance of e-commerce: Online shoppers in China. *Information & Management, 46*, 294–301.