Association for Information Systems
AIS Electronic Library (AISeL)

WISP 2018 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

Winter 12-13-2018

Why Do Users Continue to Use Mobile Cloud Computing Applications? A Security-Privacy

Hamid Reza Nikkhah
University of Arkansas, Fayetteville

Varun Grover
University of Arkansas, Fayetteville

Rajiv Sabherwal
University of Arkansas, Fayetteville

Why Do Users Continue to Use Mobile Cloud Computing Applications? A Security-Privacy Investigation

Hamid Reza Nikkhah[1]
Sam M. Walton College of Business, University of Arkansas, Fayetteville, AR, USA

Varun Grover
Sam M. Walton College of Business, University of Arkansas, Fayetteville, AR, USA

Rajiv Sabherwal
Sam M. Walton College of Business, University of Arkansas, Fayetteville, AR, USA

ABSTRACT

Mobile cloud computing (MCC) apps are mobile apps that use cloud computing technology to provide larger storage capacity and simultaneous access from different mobile devices. Despite the benefits, sending data to the cloud raises security and privacy concerns as mobile users do not have direct control over their data in the cloud. Further, many MCC apps are not used just after single use. In this study, we do a cost/benefit analysis based on security and privacy to investigate the factors that drive or inhibit mobile users to continue to use MCC apps. Additionally, we examine whether security and privacy interventions of MCC apps providers influence the cost/benefit analysis. The results of the survey with 412 MCC apps users show that while security concerns inhibit, privacy concerns do not stop using MCC apps. The value of MCC apps is the main enabler followed by trust to continue to use the apps. The results also show that security and privacy interventions do not add value to MCC apps, but they increase trust. These interventions decrease privacy concerns but have no effect on security concerns. Finally, these interventions indirectly drive users to continue to use the apps through trust.

Keywords: mobile apps, cloud computing, security, privacy, privacy calculus

[1] Corresponding author. HNikkhah@walton.uark.edu +1 479 575 4322

INTRODUCTION

Individuals share their lives, access online information, and do their businesses on the move thanks to mobile technologies. The use of mobile devices such as smartphones and tablets has been increasing over the past few years (eMarketer 2016) and individuals spend a great amount of time using mobile apps. The growing use of mobile apps to transfer and storage information provokes several challenges. First, mobile users need to access the same data through multiple devices and if data are locally stored on a mobile device, accessing the data from another device which might have another operating system would be a challenge. Additionally, the proliferation and diversity of mobile apps have caused mobile users to input more data on mobile devices, which requires larger storage capacity than the mobile devices currently possess. To meet these mobile users' needs, mobile apps developers acquire cloud computing technology and shift from native mobile apps that locally store data on mobile devices to mobile cloud computing (MCC) apps[2] that reside on mobile devices but send data automatically to the cloud (Dinh et al. 2013).

MCC apps have several unique beneficial features that cause mobile apps providers to develop many internet-based native mobile apps as MCC apps[3]. First, MCC apps are multiplatform and support almost all popular operating systems (Android, iOS, Windows, and Linux) and allow simultaneous access to data, which is necessary for collaborative projects (e.g., Google Docs). Second, data on MCC apps can be saved on mobile devices in addition to storing in the cloud (e.g., Skype). Third, MCC apps are also accessible through the web (e.g., Dropbox),

[2] Some of well-known MCC apps are Snapchat (photo sharing), Dropbox (file storage), Evernote (note taking), Viber (instant messaging), and Skype (voice and video calling). Each of these apps are multiplatform and have versions for Android, iOS, Windows, and Web.

[3] For example, Skype which was a native internet-based app finally moved to the cloud in 2016 to benefit from cloud computing technology and provide a consistent way to deliver the app to Windows XP, Windows 7, Windows 10, iOS, Android, Google Chromebooks, and Linux users (Bright 2016; Weinberger 2016).

which provides instant access to the app and data without installing the app[4]. Finally, users' data are backed up automatically by MCC apps providers without users' notice.

Despite MCC apps benefits, users have shown their concerns about the transfer of their data to the cloud. For example, users do not know where their information is sent to, who else can access their data in the remote locations (cloud), and whether their information is used for other purposes without their permissions (Pearson et al. 2009; Sun et al. 2011). Data breaches, data loss, compromising credentials, and security attacks are other concerns about using these apps (Adams 2017). These concerns found to be among the reasons why mobile users abandon using mobile apps just after a single use (Levenson 2016). Thus, it is essential for mobile apps developers to better understand mobile users' concerns and retain their users by decreasing the influential concerns.

Against this backdrop, prior studies investigate individuals' security and privacy issues of cloud computing applications and services[5]. However, previous research does not examine individuals' concerns *after* using cloud computing applications, especially MCC apps, and whether security and privacy concerns inhibit users to continue to use such apps. Moreover, as MCC apps providers create security and privacy interventions to notify users about their security and privacy practices, prior research does not study whether these interventions are effective to decrease users' concerns after adopting the apps. Consequently, the research questions of this study are: (1) what are inhibitors and drivers to continue to use MCC apps? We also investigate whether the MCC apps providers' security and privacy interventions effectively influence mobile users, by asking (2) do MCC apps providers' security and privacy interventions decrease individuals' concerns and increase the benefits of using MCC apps? To answer these research

[4] This feature is especially helpful when the mobile device is broken, and the user urgently needs to access and work with their data.
[5] Table 1 in LITERATURE REVIEW provides more information about these studies.

questions, this study adopts privacy calculus model to do a cost/benefit analysis and extends it by incorporating security and the utility and hedonic benefits underlying MCC apps value. This study is expected to provide several important contributions to mobile and cloud computing security and privacy research.

First, the privacy and security research on MCC apps predominantly provides technical solutions to address the relevant issues and the behavioral aspect of this phenomenon has received little attention. To the best of our knowledge, this is the first study that investigates the drivers and inhibitors of using MCC apps after downloading such apps. Second, prior studies argue security and privacy jointly affect mobile users to adopt MCC apps (e.g., Takabi et al. 2010). In this study, we separate security and privacy concerns to examine if either affects mobile users to continue to use MCC apps. Finally, MCC apps providers signal mobile users to assure the safety of their apps by creating security and privacy interventions. We investigate the impact of MCC apps providers' security and privacy interventions on mobile users' perceptions and whether they are effective as MCC apps providers expect.

The paper begins with reviewing literature of cloud computing applications security and privacy and privacy calculus to identify the main findings of this area. Afterward, the research model based on the extended privacy calculus model is presented. Then, we analyze the research model using partial least squares (PLS) with data from 412 MCC apps users. The paper concludes with a discussion of theoretical and practical implications.

LITERATURE REVIEW

Cloud Computing Security and Privacy

Prior cloud computing studies argue security and privacy issues of the cloud user, the cloud provider, and the relationship between the cloud user and provider from different perspectives. These studies fall into five categories: (a) cloud computing general security and

privacy issues, (b) cloud computing security and privacy design and architecture, (c) cloud computing security and privacy regulation, (d) cloud computing data security and privacy, and (e) the effect of cloud computing security and privacy beliefs. Table 1 shows the main streams of cloud computing security and privacy studies which have different objectives and focuses.

Table 1. Security and Privacy Cloud Computing Research Streams

Research Stream	Objective	Focus	Studies
General security and privacy issues	Enumerating various security and privacy challenges in cloud computing such as identity management and authentication.	Conceptual/ Technical	Pearson et al. (2009); Sun et al. (2011); Takabi et al. (2010); Zhou et al. (2010)
Security and privacy design and architecture	Providing architects and designs to develop a secure cloud computing infrastructure.	Technical	Alruwaili and Gulliver (2014); Pearson (2009); Sharma et al. (2013)
Security and privacy regulation	Discussing and examining how regulations, contracts, and agreements can decrease security and privacy concerns.	Conceptual	Kerr and Teng (2010); Mather et al. (2009); Svantesson and Clarke (2010)
Data security and privacy	Investigating how data should be stored and retained in cloud computing in a secure and private manner.	Technical	Chen and Zhao (2012); Khan and Hamlen (2012)
Security and privacy beliefs	Examining the effect of security and privacy beliefs on individuals' attitudes and behaviors.	Behavioral	Alsmadi and Prybutok (2018); Arpaci et al. (2015); Burda and Teueberg (2014)

Privacy Calculus

Privacy researchers argue that individuals do a cost/benefit analysis before disclosing information. Based on the cost/benefit analysis, individuals share their private information with third-parties in online settings when the cumulative benefits that individuals gain with disclosing information outweigh the associated cumulative costs (Dinev and Hart 2006). Privacy calculus is a cognitive/mental analysis that harmonizes the competing forces stemming from the benefits of information sharing and the costs of not withholding information (Cavusoglu et al. 2016). As Table 2 shows, privacy calculus has been used in IS privacy studies to do a privacy cost/benefit analysis by identifying privacy inhibitors and drivers in different contexts.

Table 2. Prior Privacy Calculus Studies

Study	Context	Inhibitors	Drivers	Behavior
Keith et al. (2016)	Mobile applications	General privacy concerns, Perceived privacy risk	Perceived usefulness, Perceived ease of use	Intention to adopt/disclose, Willingness to pay
Krasnova et al. (2012)	Social networking sites	Privacy concerns	Enjoyment, Trust	Self-disclosure
Liao et al. (2011)	Online transactions	Privacy concerns, Perceived risk	Trust	Intention to transact, Intention to retrieve privileged information
Li et al. (2010)	E-commerce transaction	Privacy risk belief	Perceived usefulness, Monetary rewards	Behavioral intention
Xu et al. (2009)	Location-based services	Perceived risks	Loanability, Personalization	Intention to disclose personal information
Dinev and Hart (2006)	E-commerce transaction	Perceived privacy risk, Perceived privacy concerns	Trusting beliefs, Personal interest	E-commerce use
Dinev et al. (2006)	E-commerce transaction	Perceived risk, Perceived privacy concerns	Institutional Trust	Willingness to provide personal information

RESEARCH MODEL AND HYPOTHESES DEVELOPMENT

Mobile users download and install MCC apps for different purposes. For example, mobile users download MCC games for entertainment and MCC storage and archiving apps to save data. However, regardless of the reason to use MCC apps, these apps share the same feature of sending the users' data to the cloud (Dinh et al. 2013). Thus, we focus on this shared feature of MCC apps and do not differ MCC apps in this study. To better understand the cost/benefit analysis of mobile users after using MCC apps, we adopt privacy calculus model and extend it by incorporating security and MCC apps value. We also examine whether MCC apps providers' interventions impact the cost/benefit analysis. Figure 1 shows MCC apps providers' interventions influence cost/benefit analysis and users' perceptions determine behavioral intentions.

Based on the relationships of interventions, perceptions, and behaviors, we investigate security concerns and privacy concerns as the inhibitors and MCC apps value and trust as the drivers of using MCC apps during cost/benefit analysis as depicted in Figure 2. We also include age, gender, perceived ease of use, and prior MCC apps use as the control variables in the research model.

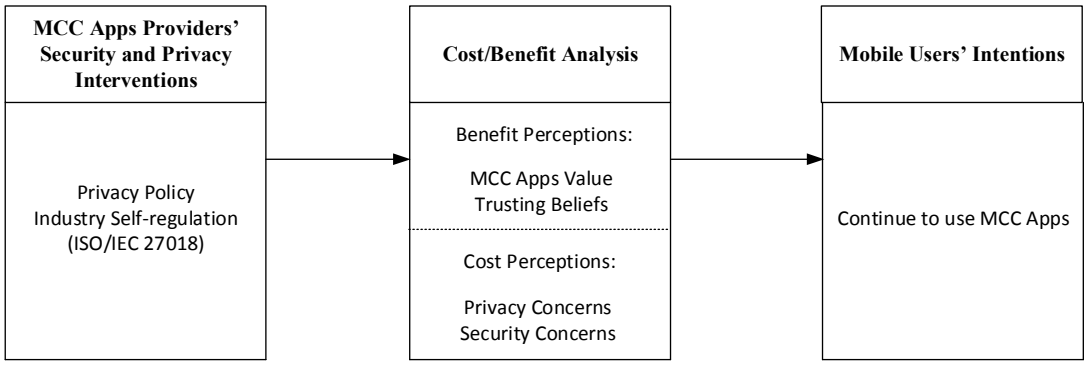

Figure 1. Conceptual Model

Perceived MCC Apps Value

Mobile users download MCC apps from different categories such as education, game, health, utility, and travel etc. Each MCC app from any category is designed for providing utilitarian benefits or hedonic benefits or a combination of both to mobile users. In this regard, prior research argues that, in the mobile context, utilitarian and hedonic beliefs drive users' behaviors (Wakefield and Whitten 2006). Perceived MCC apps value refers to what extent users believe that MCC apps that send users' data to the cloud provide benefits. After downloading, users evaluate the value of mobile apps based on utilitarian and hedonic benefits to find whether it is worthwhile to keep and use the apps. Thus, if any specific app does not provide enough value based on a combination of utilitarian and hedonic benefits from a user's perspective, the user removes the apps from the mobile device. Previous research also finds that utilitarian benefits and hedonic benefits are the main determinants of IS continuance (e.g., Li et al. 2015). Hence, we hypothesize:

H1: Perceived MCC apps value has a positive effect on continue to use MCC apps.

Trust

Trust plays a key role in any exchange between two parties, especially in an online transaction context (Dinv and Hart 2006). It facilitates an online transaction by encouraging the

parties to disclose information to each other. Mayer et al. (1995) define trust as "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party." Trust has been used in a number of privacy calculus models as the benefit of disclosing information or using a system. Dinev and Hart (2006) argue trust is one of the "confidence and enticement" beliefs and propose a privacy calculus model in which trust positively affects willingness to provide personal information to transact on the internet. In mobile apps context, a recent survey with more than 6500 mobile users from 10 countries finds that the lack of trust is the main obstacle to greater use of mobile apps and prevents users from downloading and using apps (Mobile Ecosystem Forum 2017). Similarly, we argue that when mobile users have trust to MCC apps providers, they believe the providers do not behave maliciously and their personal information is safe in the cloud. hypothesize:

H2: Trust has a positive effect on continue to use MCC apps.

Perceived Privacy Concerns

Privacy concerns on the internet are about users' information gathering, storing, and analyzing without their awareness and permission. When users input information on MCC apps their information is transferred and stored in the cloud where users do not have direct control over their data. In fact, the main privacy concern about using any cloud computing applications is the lack of control over the information sent to the cloud for storage and process (Sun et al. 2011).

Perceived privacy concerns in this study refer to the concerns about any opportunistic behavior that MCC apps providers can perform with the mobile users' data. In addition to the lack of direct control, data theft and unauthorized modification in the cloud are other privacy

concerns about using MCC apps (Pearson et al. 2009). MCC apps can steal the users' data stored on the mobile devices (e.g., photos and contacts) and secretively track users' location. All these concerns make mobile users reluctant to use MCC apps further. Moreover, IS privacy research also finds the negative effect of perceived privacy concerns on users' behavior in other contexts, such as online transaction (Dinev and Hart 2006; Dinev et al. 2006) and social networking sites (Krasnova et al. 2012). Thus, we hypothesize:

H3: Perceived privacy concerns have a negative effect on continue to use MCC apps.

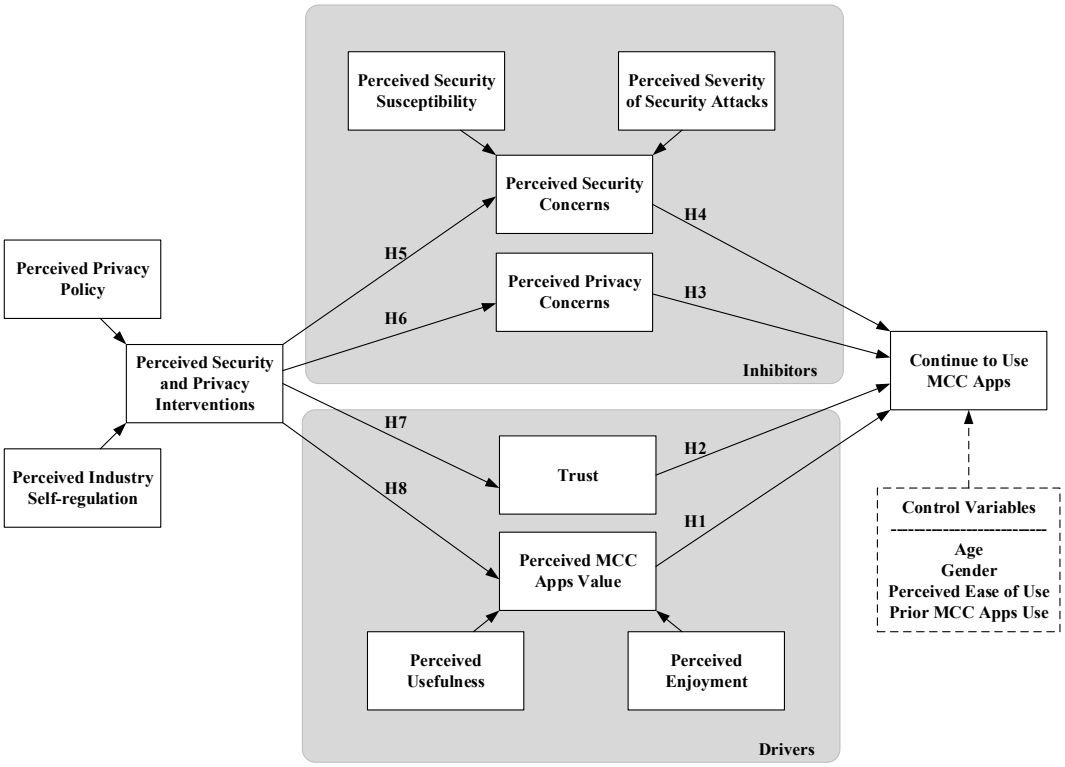

Figure 2. Research Model

Perceived Security Concerns

Mobile users need to connect to the internet for using MCC apps as these apps require to connect to the cloud through the internet, which makes security one of the major issues of using MCC apps. Perceived security concerns refer to the probability that users' information will be

read and manipulated by unauthorized parties during transfer or storage in the cloud. While privacy concerns are about the intentional opportunistic behavior of MCC apps providers, security concerns are about the external threats to the safety of MCC apps, the communication between MCC apps and the cloud, and the cloud infrastructure (Rahimi et al. 2014; Ali et al. 2015). Mobile devices are exposed to security threats like malicious codes (e.g., virus, worms, Trojan horse, and spyware) by installing MCC apps, and hackers can use these codes to hack mobile devices (Ashford 2015). However, protecting mobile devices against such threats is more difficult than resourceful devices such as PC (Dinh et al. 2013). The security of communication between MCC apps and the cloud is another concern about using MCC apps because this communication can face threats such as denial-of-service, man-in-the-middle, eavesdropping, IP-spoofing based flooding, and masquerading (Ali et al. 2015).

Prior IS research extensively finds that security concerns arouse users' behaviors (e.g., Anderson and Agarwal 2010; Johnston et al. 2015). Chen and Zahedi (2016) find that concerns about online security threats lead to coping behaviors such as avoidance. Likewise, mobile users react to their concerns about the security of MCC apps and we believe that security concerns are another major factor to stop using MCC apps and we hypothesize:

H3: Security privacy concerns have a negative effect on continue to use MCC apps.

Security and Privacy Interventions

With the growing concerns about online information disclosure, online companies attempt to assure users that data transaction and storage are safe, and they protect users' data against security and privacy threats. Online companies can reduce the disutility caused by data collection if they commit to use data responsibly and convey this commitment through security and privacy interventions (Hui et al. 2007). Security and privacy interventions are the signals that online companies give to users to convey their efforts to protect users' data.

MCC apps providers make security and privacy interventions to show their fair information practices in the cloud. Prior studies mention that two common interventions are privacy policy and industry self-regulation (Xu et al. 2011) which are adopted by MCC apps providers too. MCC apps providers create privacy policies include information about not only privacy practices but also security practices and how technical security solutions can protect data in the cloud[6]. MCC apps providers (e.g., Microsoft, Dropbox, Amazon) have also adopted international standard ISO/IEC 27018 as another intervention to assure users of information safety in the cloud. We believe that when users encounter the providers' security and privacy interventions, they are informed about security and privacy protections and their concerns to use MCC apps decrease. Thus, we hypothesize:

H5: Security and privacy interventions decrease security concerns.

H6: Security and privacy interventions decrease privacy concerns.

Security and privacy interventions are the cues to show that online companies are honest, and they do not behave opportunistically. Bansal et al. (2015) argue that users seek to form the correct trust attitude in online providers by relying on assurance mechanisms. When users encounter security and privacy interventions, they assume the online provider cares about the safety of their information and they become vulnerable to the provider's actions. As a result, assurance mechanisms that include various security and privacy interventions found to be effective to build trust (Wu et al. 2012). Moreover, prior research argues that when users disclose more information, they receive more personalized services (Li and Unger 2012), which helps the users to get most of MCC apps functionality. For example, providing more information to MCC apps after installation enables games to give an option that game players choose with whom they

[6] Viber provides information about security by mentioning "*We maintain technical, physical, and administrative security measures to protect the security of your personal information against loss, misuse, unauthorized access, disclosure, or alteration. Some of the safeguards we use include firewalls, data encryption, physical access controls to our data centers and information access authorization controls...*" (Viber Privacy Policy 2018).

play based on users' profile or health and lifestyle apps to send better health hints based on the users' personal information. With these two perspectives put forward, we hypothesize:

H7: Security and privacy interventions increase trust.

H8: Security and privacy interventions increase MCC apps value.

METHODOLOGY

We conducted a web-based survey in the USA in 2018 to reach a wide range of MCC apps users. At the beginning of the survey, we explained what MCC apps are by providing examples from well-known apps. Before the primary study, we did a pilot study with 30 similar respondents to our primary study participants to solicit feedback. We encouraged study participation by a small monetary incentive for primary study. Then, we removed the responses completed in less than 5 minutes based on the pilot study feedback and detected and removed outliers from our study (Chatterjee and Hadi 1986) to increase the quality of data. As a result, we reached 412 acceptable responses for further analyses. Demographics of participants show that 47% were female, 51% were 18-34 years old, 42% used internet for 16-20 years, and 70% used MCC apps for 6 years and under. We adapted the items of constructs by reviewing literature[7]. Following Petter et al.'s (2007) rules to decide on formative or reflective measurement, we found that all the second-order constructs of our research model are formative. All the items of the survey are based on a 7-point Likert scale.

Reliability, Validity, and Common Method Variance

We checked the reliability and validity of constructs before conducting further analyses. Table 2 demonstrates the means, standard deviations, and reliabilities of the measures as well as

[7] We adapted the items of continue to use MCC apps from Bhattacherjee (2001), trust and perceived privacy concerns from Dinev and Hart (2006), perceived security susceptibility and perceived severity of security attacks from Chen and Zahedi (2016), perceived usefulness from Davis (1989), perceived enjoyment from van der Heijden (2004), perceived privacy policy and perceived industry self-regulation from Xu et al. (2011), and prior MCC apps use by asking "how long have you been using MCC apps?".

the inter-variable correlations. The results confirm the reliability and validity of constructs[8] (Table 2). For each formative construct, we found the variance inflation factor (VIF) was below 2.0, and the weight range of the associated indicators was significant.

Table 2. Descriptives, Reliabilities, Average Variance Extracted, and Correlations

Variable	Mean	S.D.	AVE	α	AGE	GEN	EXP	EASE	INT	VAL	TRUST	PRI	SEC	CONT
AGE	36.99	12.12	N/A	N/A	**1.00**									
GEN	0.54	0.49	N/A	N/A	0.07	**1.00**								
EXP	5.54	3.17	N/A	N/A	-0.10*	-0.06	**1.00**							
EASE	5.68	0.99	0.79	0.91	-0.07	-0.03	0.16**	**0.89**						
INT	4.39	1.16	N/A	N/A	0.03	0.01	-0.05	0.10*	**0.77**					
VAL	5.09	0.84	N/A	N/A	-0.05	-0.06	0.15**	0.48***	0.32***	**0.73**				
TRUST	4.45	1.22	0.80	0.92	0.10*	-0.02	-0.04	0.13**	0.67***	0.30***	**0.90**			
PRI	4.92	1.44	0.88	0.95	0.02	0.00	0.00	-0.04	-0.26***	-0.13**	-0.43***	**0.94**		
SEC	4.56	1.07	N/A	N/A	0.00	0.05	0.02	-0.12*	-0.23***	-0.09	-0.39***	0.53***	**0.79**	
CONT	5.53	1.04	0.88	0.95	0.00	0.00	0.24***	0.41***	0.31***	0.67***	0.38***	-0.25***	-0.25***	**0.94**

*Notes. Diagonal is square root of average variance extracted (AVE). * $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$. S.D. = standard deviation; α = Cronbach alpha; CR = composite reliability; GEN = Gender; Experience = Prior MCC apps use; EASE = perceived ease of use; INT = Perceived security and privacy interventions; Value = perceived MCC apps value; PRI= perceived privacy concerns; SEC = perceived security concerns; CONT = continue to use MCC apps.*

Before testing hypotheses, we investigated whether our study suffers from common method bias by running Harmon's one-factor test[9] to find whether one component, in expletory factor analysis, explains 50 percent of the model or only one single factor appears[10] (Podsakoff and Organ 1986) and Lindel and Whitney's (2001) *marker variable* test[11]. Based on the results of these two tests, we found that common method bias is not an issue in this study.

RESULTS AND DISCUSSION

We used partial least squares (PLS) to test the hypotheses because PLS is well-suited for testing the models with formative constructs and maximizing variance explained (Cenfetelli and

[8] Values of Cronbach alpha (α) are above .7, those of average variance extracted (AVE) are above .5, and all inter-variable correlations are below the square root of the variable' AVE value.

[9] Although there are critics against using Harmon's one-factor test, it is still commonly used in IS research (e.g., Goode et al. 2017).

[10] We found that the first factor could only explain 28 percent of the model variance.

[11] We used internet experience as the marker variable and found that the matrices of item-to-item correlations show non-significant correlations (ranging from -0.02 to 0.08) with the nine variables of the measurement model.

Bassellier 2009; Dijkstra and Henseler 2015). Figure 3 shows PLS results and the significant path coefficients. As you can see in Figure 3, MCC apps value (b= 0.55, p < 0.001) and trust (b= 0.14, p < 0.01) are considered effective enablers as they positively impact continue to use MCC apps. Thus, H1 and H2 are supported. Therefore, increasing the value of MCC apps by enhancing utility and hedonic features of the app should be the priority of MCC apps providers. Trust has been shown to encourage users to disclose information in online settings (Dinev and Hart 2006) and we found that, in MCC apps context, trust is also a driver to disclose information after adopting the apps.

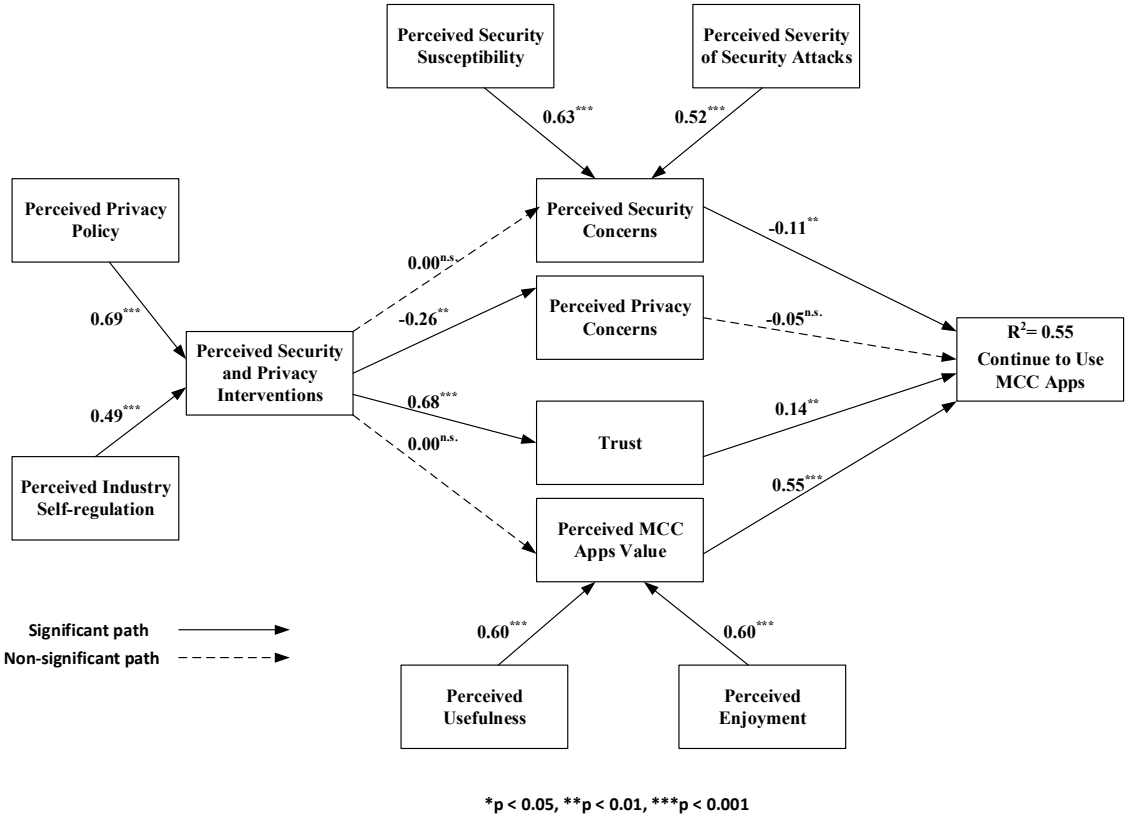

Figure 3. PLS Results

However, the constructs that are the inhibitors of continue to use MCC apps have different influences on mobile users. The results show that perceived privacy concerns (b= -0.05, p = 0.14) is not a significant factor to stop mobile users using MCC apps. Thus, H3 is not supported. This result is interesting as the prior studies of MCC apps studies emphasize that

privacy concern is a major obstacle to use these apps (e.g., Arpaci et al. 2015; Pearson et al. 2009; Sun et al. 2011). However, we found that after installation of MCC apps, mobile users do not have privacy concerns, or these concerns are not strong enough to stop mobile users working with MCC apps.

Mobile users have security concerns after downloading and installing MCC apps because the results reveal that perceived security concerns ($b= -0.11$, $p < 0.01$) negatively affect continue to use MCC apps. As a result, H4 is supported in this study. The results confirm that, after using MCC apps, mobile users are not concerned about the opportunistic behavior of the providers, but they have concerns about the external threats from the internet (e.g., hackers) that can read and manipulate the users' data during the communication or after storing in the cloud. Consequently, MCC apps providers should design various methods to signal mobile users that the communication with the cloud data and data storage are secure enough so that they can retain their users.

We found that security and privacy interventions can play a role to influence mobile users' perceptions. These interventions can positively affect the drivers and negatively impact the inhibitors of continue to use MCC apps. Yet, Figure 3 demonstrates that security and privacy interventions influence specific factors of cost and benefit analysis. Results show security and privacy interventions ($b= 0.00$, $p < 0.53$) do not decrease security concerns, but they significantly decrease ($b= -0.26$, $p < 0.01$) privacy concerns. Thus, H5 is not supported, but H6 is supported in this study. This finding is important for MCC apps providers because they invest in creating security and privacy interventions and these interventions are able to decrease only privacy concerns that are not influential to keep users. Security and privacy interventions can substantially increase trust to MCC apps as the results reveal that these interventions ($b= 0.68$, $p < 0.001$) have a positive effect on trust. Thus, H7 is supported.

On the other hand, security and privacy interventions (b= 0.00, p = 0.98) do not have a significant effect on perceived MCC apps value and cannot add any value to the current value of the app from mobile users' perspective. The results of testing the effect of control variables show that age (b= 0.04, p = 0.16), gender (b= 0.04, p = 0.14), and perceived ease of use (b= 0.08, p = 0.05) did not have a significant effect on the dependent variable. Prior MCC apps use (b= 0.16, p < 0.001) affected continue to use MCC apps, which indicates the more users work with MCC apps, the more likely they continue to use these apps and MCC apps providers should invest in useful and fun features more than the features that make the apps ease of use. Finally, the results confirm the research model (R^2= 0.55) has a reasonable explanatory power.

Post-hoc Analyses

We conducted several post-hoc analyses to investigate more the relationships of the research model. The results of t-test (t= 6.44, p < 0.001) show the path coefficients of perceived MCC apps value and trust are significantly different and we can conclude that MCC apps value is the main enabler of continuing to use MCC apps. The results (t= 6.81, p < 0.001) show that security and privacy interventions affect trust more than perceived privacy concerns. Finally, the results show that security and privacy interventions (b= 0.11, p <0.001) have a significant *indirect* effect on continue to use MCC apps through trust.

CONCLUSION

In this study, we analyzed the survey of 412 MCC apps users to find whether security and privacy concerns inhibit and MCC apps value and trust drive mobile users to continue to use MCC apps based on an extended privacy calculus model. We found *only* security concerns inhibit and MCC apps value and trust drive users to continue to use MCC apps. We also found that security and privacy interventions partially affect cost/benefit analysis and have a positive effect on trust, and a negative effect on privacy concerns.

REFERENCES

Adams, C. 2017. "Top Cloud Data Security Risks, Threats, And Concerns." (https://blog.panoply.io/top-cloud-security-threats-risks-and-concerns/, accessed July 12, 2018)

Ali, M., Khan, S. U., and Vasilakos, A. V. 2015. "Security in Cloud Computing: Opportunities and Challenges," *Information Sciences* (305), pp. 357-383.

Alruwaili, F. F., and Gulliver, T. A. 2014. "ISPC: An Information Security, Privacy, and Compliance Readiness Model for Cloud Computing Services," *International Journal of Future Generation Distributed Systems* (4:4), pp. 1-11.

Alsmadi, D., and Prybutok, V. 2018, "Sharing and Storage Behavior via Cloud Computing: Security and Privacy in Research and Practice," *Computers in Human Behavior* (85), pp. 218-226.

Anderson, C. L., and Agarwal, R. 2010. "Practicing Safe Computing: A Multimedia Empirical Examination of Home Computer User Security Behavioral Intentions," *MIS Quarterly* (34:3), pp. 613-643.

Arpaci, I., Kilicer, K., and Bardakci, S. 2015. "Effects of Security and Privacy Concerns on Educational Use of Cloud Services," *Computers in Human Behavior* (45), pp. 93-98.

Ashford, W. 2015. "Hackers Can Exploit Free Mobile Apps to Steal Data, Study Shows" (https://www.computerweekly.com/news/2240237515/Hackers-can-exploit-free-mobile-apps-to-steal-data-study-shows/, accessed September 8, 2018)

Bansal, G., Zahedi, F. M., and Gefen, D. 2015. "The Role of Privacy Assurance Mechanisms in Building Trust and the Moderating Role of Privacy Concern," *European Journal of Information Systems* (24:6), pp. 624-644.

Bright, P. 2016. "Skype Finalizes Its Move to the Cloud, Ignores the Elephant in the Room" (https://arstechnica.com/information-technology/2016/07/skype-finalizes-its-move-to-the-cloud-ignores-the-elephant-in-the-room/, accessed October 12, 2018)

Burda, D., and Teuteberg, F. 2014. "The Role of Trust and Risk Perceptions in Cloud archiving—Results from an Empirical Study," *The Journal of High Technology Management Research* (25:2), pp. 172-187.

Cavusoglu, H., Phan, T. Q., Cavusoglu, H., Airoldi, E. D. 2016. "Assessing the Impact of Granular Privacy Controls on Content Sharing and Disclosure on Facebook," *Information Systems Research* (27:4), pp. 848–879.

Cenfetelli, R. T., and Bassellier, G. 2009. "Interpretation of Formative Measurement in Information Systems Research," *MIS Quarterly* (33:4), pp. 689-707.

Chen, D., and Zhao, H. 2012. "Data Security and Privacy Protection Issues in Cloud Computing," In *Proceedings of* IEEE International *Computer Science and Electronics Engineering (ICCSEE),* pp. 647-651.

Chen, Y., and Zahedi, F. M. 2016. "Individuals' Internet Security Perceptions and Behaviors: Polycontextual Contrasts Between the United States and China." *MIS Quarterly* (40:1), pp. 205-222.

Davis, F. D. 1989. "Perceived Usefulness, Perceived Ease of use, and User Acceptance of Information Technology," *MIS Quarterly* (13:3), pp. 319-340.

Dijkstra, T. K., and Henseler, J. 2015. "Consistent Partial Least Squares Path Modeling." *MIS Quarterly* (39:2), pp. 297-316.

Dinev, T., and Hart, P. 2006. "An Extended Privacy Calculus Model for e-Commerce Transactions," *Information Systems Research* (17:1), pp. 61-80.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., and Colautti, C. 2006. "Privacy Calculus Model in E-Commerce–A Study of Italy and the United States," *European Journal of Information Systems* (15:4), 389-402.

Dinh, H. T., Lee, C., Niyato, D., and Wang, P. 2013. "A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches," *Wireless Communications and Mobile Computing* (13:18), pp. 1587-1611.

eMarketer. 2016. "US Internet Users Rely on Mobile Devices for Digital Access." (https://www.emarketer.com/Article/US-Internet-Users-Rely-on-Mobile-Devices-Digital-Access/1013649/, accessed August 8, 2018)

Goode, S., H. Hoehle, V. Venkatesh, and S. A. Brown. 2017. "User Compensation as a Data Breach Recovery Action: An Investigation of the Sony PlayStation Network Breach." *MIS Quarterly* (41:3), pp. 703-727.

Hui, K., Teo, H. H., and Lee, S. T. 2007. "The Value of Privacy Assurance: An Exploratory Field Experiment," *MIS Quarterly* (31:1), pp. 19-33.

Johnston, A. C., Warkentin, M., and Siponen, M. 2015. "An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to The Human Asset Through Sanctioning Rhetoric," *MIS Quarterly* (39:1), pp. 113-134.

Keith, M. J., Babb, J., Lowry, P. B., Furner, C., and Abdullat, A. 2016. "Limited Information and Quick Decisions: Consumer Privacy Calculus for Mobile Applications," *AIS Transactions on Human-Computer Interaction* (8:3), pp. 88-130.

Kerr, J., and Teng, K. 2012. "Cloud Computing: Legal and Privacy Issues," *Journal of Legal Issues and Cases in Business* (1:1), pp. 1-11.

Khan, S. M., and Hamlen, K. W. 2012. "AnonymousCloud: A Data Ownership Privacy Provider Framework in Cloud Computing," In *Proceedings of 11th IEEE International Trust, Security and Privacy in Computing and Communications*, pp. 170-176.

Krasnova, H., Veltri, N. F., and Günther, O. 2012. "Self-Disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture," *Business & Information Systems Engineering* (4:3), pp. 127-135.

Levenson, H. 2016. "7 Common Reasons Users are Abandoning your App." (https://www.webanalyticsworld.net/2016/08/why-users-are-abandoning-your-mobile-app.html/ accessed August 8, 2018)

Li, H., Liu, Y., Xu, X., Heikkilä, J., and Van Der Heijden, H. 2015. "Modeling Hedonic IS Continuance Through the Uses and Gratifications Theory: An Empirical Study in Online Games," *Computers in Human Behavior*, 48, pp. 261-272.

Li, H., Sarathy, R., and Xu, H. 2010. "Understanding Situational Online Information Disclosure as a Privacy Calculus," *Journal of Computer Information Systems* (51:1), pp. 62-71.

Li, T., and Unger, T. 2012. "Willing to Pay for Quality Personalization? Trade-Off between Quality and Privacy," *European Journal of Information Systems* (21:6), pp. 621-642.

Liao, C., Liu, C., and Chen, K. 2011. "Examining the Impact of Privacy, Trust and Risk Perceptions Beyond Monetary Transactions: An Integrated Model," *Electronic Commerce Research and Applications* (10:6), pp. 702-715.

Lindell, M. K., and Whitney, D. J. 2001. "Accounting for Common Method Variance in Cross-Sectional Research Designs." *Journal of Applied Psychology* (86:1), pp. 114-121.

Mather, T., Kumaraswamy, S., and Latif, S. 2009. *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance,* O'Reilly Media, Inc.

Mayer, R. C., Davis, J. H., and Schoorman, F. D. 1995. "An Integrative Model of Organizational Trust," *Academy of Management Review* (20:3), pp. 709-734.

Mobile Ecosystem Forum. 2017. "Global Consumer Trust Report 2017". (https://mobileecosystemforum.com/programmes/consumer-trust/global-consumer-trust-survey-2017/, accessed October 5, 2018)

Pearson, S. 2009. "Taking Account of Privacy when Designing Cloud Computing Services," In *Proceedings of ICSE Workshop on Software Engineering Challenges of Cloud Computing*, pp. 44-52.

Pearson, S., Y. Shen, and M. Mowbray. 2009. "A Privacy Manager for Cloud Computing," In *Proceedings of IEEE International Conference on Cloud Computing*, Springer Berlin Heidelberg, pp. 90-106.

Petter, S., Straub, D. and Rai, A. 2007. "Specifying Formative Constructs in Information Systems Research," *MIS Quarterly* (31:4), pp. 623-656.

Podsakoff, P. M., and Organ, D. W. 1986. "Self-Reports in Organizational Research: Problems and Prospects," *Journal of Management* (12:4), pp. 531-544.

Rahimi, M. R., Ren, J., Liu, C. H., Vasilakos, A. V., and Venkatasubramanian, N. 2014. "Mobile Cloud Computing: A Survey, State of Art and Future Directions," *Mobile Networks and Applications* (19:2), pp. 133-143.

Sharma, S., and Khiva, N. K. 2013. "Secure Cloud Architecture for Preserving Privacy in Cloud Computing Using OTP/WTP," *Global Journal of Computer Science and Technology* (13:3), pp. 15-18.

Sun, D., Chang, G., Sun, L., and Wang, X. 2011. "Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments," *Procedia Engineering* (15), pp. 2852-2856.

Svantesson, D., and Clarke, R. 2010. "Privacy and Consumer Risks in Cloud Computing," *Computer Law & Security Review* (26:4), pp. 391-397.

Takabi, H., Joshi, J. B., and Ahn, G. 2010. "Security and Privacy Challenges in Cloud Computing Environments," *IEEE Security & Privacy* (8:6), pp. 24-31.

Van der Heijden, H. 2004. "User Acceptance of Hedonic Information Systems," *MIS Quarterly* (28:4), pp. 695-704.

Viber Privacy Policy. 2018. (https://www.viber.com/terms/viber-privacy-policy/, accessed August 7, 2018)

Wakefield, R. L., and Whitten, D. 2006. "Mobile Computing: A User Study on hedonic/utilitarian Mobile Device Usage," *European Journal of Information Systems* (15:3), pp. 292-300.

Weinberger, M. 2016. "Your Skype Calls Are About to Get Much Better" (https://www.businessinsider.com/microsoft-skype-moves-to-cloud-2016-7/, accessed October 7, 2018)

Wu, K., Huang, S. Y., Yen, D. C., and Popova, I. 2012. "The Effect of Online Privacy Policy on Consumer Privacy Concern and Trust," *Computers in Human Behavior* (28:3), pp. 889-897.

Xu, H., Dinev, T., Smith, J., and Hart, P. 2011. "Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances," *Journal of the Association for Information Systems* (12:12), pp. 798-824.

Xu, H., Teo, H., Tan, B. C. and 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), pp. 135-174.

Zhou, M., Zhang, R., Xie, W., Qian, W., and Zhou, A. 2010. "Security and Privacy in Cloud Computing: A Survey," In *Proceedings of 6th International Conference on Semantics Knowledge and Grid*, pp. 105–112.