Journal of International Technology and Information Management

Volume 24 | Issue 3 Article 3

2015

Effects of Exchange Benefits, Security Concerns and Situational Privacy Concerns on Mobile Commerce Adoption

Hua Dai
University of Winsconsin-La Crosse

Yan Chen
Auburn University at Montgomery

Effects of Exchange Benefits, Security Concerns and Situational Privacy Concerns on Mobile Commerce Adoption

Hua Dai
Information Systems Department
University of Wisconsin-La Crosse
USA

Yan Chen
Information Systems Department
Auburn University at Montgomery,
USA

ABSTRACT

Few empirical studies have examined both privacy and security concerns in the context of mobile commerce (m-commerce) while accounting for the effects of situational privacy concerns specific to the context of m-commerce. This research fills this gap in research by exploring users' exchange perceptions specific to the context of m-commerce in China and by examining the inhibitors and drives of m-commerce adoption in China from the perspectives of social exchange. Particularly, this research develops an integrated research model in which users' perceptions on value added of and usefulness of m-commerce, and users' privacy concerns and security concerns of m-commerce are examined. The research model is empirically tested by using the survey data collected in a large city in China. Our findings confirmed the conceptualization of the research model and indicated that users' perceived exchange benefits are the drivers of m-commerce use. Users' security concerns hinder their intention to conduct m-commerce. Surprisingly, users' privacy concerns seem not to have a significant impact on users' favorable attitude toward m-commerce, but situational privacy concerns including location tracking and personalized use of user information significantly impact users' general privacy concerns.

Keywords: Security, Privacy, Mobile commerce, China, USA

INTRODUCTION

Smartphone and tablet shipments worldwide were projected to reach 1.95 billion units and 320 million units respectively in 2015 (Gartner, 2014). As smartphone and other mobile devices are rapidly penetrating the world population and companies are increasing their effort to sell products and services via mobile markets, both the academia and the industry have projected a boom in mobile commerce (m-commerce) in the near future (e.g. Forrester, 2011). China, as a new engine of the world economy, has started experiencing such boom: in 2013, m-commerce reached ¥167.6 billion ($27.5 billion) and was expected to hit a trillion Yuan with an annual growth rate of 39.4% in 2017 (ChinaInternetWatch, 2014). In spite of this great penetration of mobile devices and seemingly great potential in m-commerce worldwide, m-commerce was projected to account for only 7% of Internet sales by 2016 (Forrester, 2011). It seems that users still very hesitate to engage in m-commerce. Surveys indicate that along with other barriers, privacy and security concerns may be two major hurdles to prevent users from engaging in m-commerce.

  ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

Unlike traditional e-commerce via PCs and wired Internet, m-commerce is conducted via mobile devices and the wireless Internet. Research has found that mobile computing in general is more subject to security and privacy risks (Ghosh and Swaminatha, 2001). Mobile computing tends to and is able to collect more personal data from users. For example, it is very easy to track a user's current location via his/her mobile devices, which is not a case in traditional e-commerce. Thus, the unique features of mobile computing cause different and *situational privacy concerns* in addition to *general privacy concerns* among users. A great deal of research has investigated the role of general privacy concerns in various information systems (IS) and services adoption intentions and behaviors (Dinev et al., 2013; Malhotra et al., 2002; Smith et al., 1996; Stewart & Segars, 2002). However, little research has studied situational privacy concerns with a contextual emphasis while exceptions exist (e.g. Li et al., 2003; Yun et al., 2013). Situational privacy concerns pertain to situations or domains and may have different impact on users' general privacy perception and adoption behaviors (Li et al., 2010). Past literature has identified two m-commerce specific privacy concerns including concerns about location tracking and personalized use of information and such situational privacy concerns may impact users' general privacy concerns which in turn impact users' intention to adopt and conduct m-commerce (Dai et al., 2010; Yun et al., 2013).

Moreover, mobile devices and signals roam through the air and across organization boundaries, making mobile data transmission extremely vulnerable to security risks (Ghosh & Swaminatha, 2001). Consequently, getting users to become confident in the security of m-commerce is a tough task. Indeed, users have expressed that security issues regarding mobile computing are a deterrent factor for their mobile shopping (SAP, 2013). Clearly, to increase users' willingness and intention to conduct m-commerce, a deep understanding of users' security concerns and the impact of such concerns on their m-commerce use is critical. Past research in IS has studied users' security perceptions and behaviors in the general context of the Internet (Anderson & Agarwal, 2010; Chen & Zahedi, 2009). Little research has focused on users' security concerns in the context of m-commerce. A review of the electronic commerce literature further identifies a central issue in the conceptualization of consumers' security and privacy perceptions: the extent to which privacy and security perceptions are defined as distinct concepts and the lack of understanding of how they are related. Dutta and Macrohan (2002) distinguished the concept of privacy and security and indicated that "privacy" deals with the degree of control over information about one's self; while "security" deals with information safety in terms of confidentiality, integrity and authentication. Furthermore, although security concerns and privacy concerns are separate constructs, both of them could exert significant influence on users' decision-making on their m-commerce behaviors. Thus, we argue that a better understanding of both privacy and security concerns in m-commerce could help overcome the obstacles to m-commerce and facilitate m-commerce.

Furthermore, consumers are fundamentally self-interested, value-driven. They make using vs. not using or adopting vs. not adopting decisions based on the trade-offs of rewards and costs (Zeithaml, 1988). In other words, similar to committing to other social relationships, consumers' decisions on use or transaction are based on rewards they can get while calculating the costs they have to pay for (Blau, 1964; Homans, 1958). When conducting m-commerce, while users have to bear probably more privacy and security risks, they enjoy values and conveniences, such as anywhere, anytime accesses provided by mobile computing. Thus we posit that users' decision on m-

  ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

commerce is based on the "calculus" of rewards and costs, according to the social exchange theory (Blau, 1964; Homans, 1958).

Additionally, China is experiencing a dramatic growth in mobile communication networks, mobile device penetration, and m-commerce (ChinaInternetWatch, 2014; Lu et al., 2003). Although a large portion of its population, particularly low-income population, still does not have the access to mobile devices and wireless Internet, many existing mobile users have an established comfort level with mobile devices and their functionality (Lu et al., 2004). In addition, given the current rapid growth rate, m-commerce may have an exceptional potential in the near future in China. With such potential for growth of m-commerce in China, understanding users' privacy and security concerns as well as their value perceptions is critical.

To fill the above mentioned research gaps, this study draws upon the social exchange theory (SET) (Blau, 1964; Homans, 1958) to develop a research model in which both users' reward perceptions in terms of perceived value and perceived usefulness of m-commerce, cost perceptions in terms of privacy and security concerns, and the consequent impacts of those perceptions are examined. In addition, the relationships between the general privacy concerns and situational privacy concerns are investigated.

The rest of the paper is organized as follows. The literature is reviewed and the SET which serves the theoretical foundation for the research model. Then the model and its hypotheses were developed. Then, description of the research methodology. The empirical analysis for the model and hypothesis testing results were reported. The last section discussed the research findings, implications, contributions, and limitations of the study. The directions for future studies were also outlined in this section.

LITERATURE REVIEW

General and Situational Privacy Concerns in M-Commerce

Privacy issues have been recognized by both industries and academia as one of the major concerns in the growth of e-commerce (e.g. Flavián and Guinalíu, 2006; SAP, 2013). Keeping consumers' personal information private after the information is collected for commercial purposes is viewed as a distinct consumer right from both legal and ethical perspectives. Meanwhile, it is very common that websites collect personal information from consumers for a variety of purposes such as registration, advertising and e-commerce. As a result, consumers are concerned about their privacy. A large body of research in IS has examined privacy issues in various contexts such as online shopping (Van Slyke, 2006), location based services (Xu et al., 2009; Yun et al., 2013), Web privacy statements (Gauzente, 2004), just to list a few. Most studies focused on *general security concerns* based on the conceptualization of Smith et al. (1996), which is not specific to the context of the study (Li et al., 2010). Smith et al. (1996) identified individual's concerns for privacy with four dimensions: collection, errors, secondary use, and unauthorized access. An individual would be concerned for privacy if an organization collects too much (collection) or incorrect personal data (errors), uses the data for purposes without the individual's knowledge or consent (secondary use), and has no proper access control for data (unauthorized access) (Smith et al., 1996). Thus general privacy concerns refer to an individual's worry about collection, use and error of information collected from him/her (Smith et al., 1996).

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

In the mobile environment, since the openness of the platform adds greater perceived risks for privacy violation, it is understandable that users would demand more privacy protection. So, providing users with information about how their personal data are used and addressing their privacy concerns become even more critical in their intention to conduct m-commerce (Dai et al., 2010). Past studies (e.g. Xu et al., 2009; Yun et al., 2013) have also found that general privacy concerns play an important role in mobile services and m-commerce adoption behaviors such as adopting location-based services.

While general privacy concerns are important as a determinant of various privacy related attitudes and behaviors, *situational privacy concerns* are distinct concepts pertaining to a specific situation or domain (Li et al., 2010). Situational privacy concerns have a contextual emphasis and can "unravel the intricacies of privacy concerns" (Li et al., 2010, p. 62). In the domain of mobile computing, the mobile technology provides the capability of tracking a user's specific location at a specific moment and linking collected data to the user. Thus location-tracking and personalized use of information are two major situational privacy concerns in addition to general privacy concerns in the domain of mobile computing. We argue that such situational privacy concerns may impact users' general privacy concerns which in turn impact users' intention to adopt and conduct m-commerce (Dai et al., 2010).

Security Concerns in M-Commerce

Behavioral aspects of information security have recently drawn more attention, though both the academia and the industry have traditionally focused on technical aspects of information security. Recent studies pointed out that users' security perceptions, such as security concerns, had significant influence on their behavioral intention (Chen and Dai, 2014). Past research found that security concerns about security breaches had positive, significant impacts on security policy compliance attitudes of employees in organizations (Herath and Rao, 2009). Past research also found that security concerns along with other factors such as security countermeasure response efficacy and self-efficacy increased their threat avoidance behaviors (Chen and Zahedi, 2009). In addition, Salisbury et al. (2001) found that perceived Web security, usefulness and ease of navigation had significant, positive impact on online purchase intention, and Flavián and Guinalíu (2006) found that consumers' perception of security regarding the handling of their personal data had a positive association with their trust in the web. Security concerns are defined as the extent of an individual's worry about information safety in terms of information confidentiality, integrity and authentication. Past studies focused on the general security concerns and perceptions among employees or home Internet users (Chen and Dai, 2014; Chen and Zahedi, 2009; Herath and Rao, 2009). Little research has examined security concerns as well as the consequence of the concerns in the context of m-commerce.

Social Exchange Theory

The social Exchange Theory (SET) has been applied in many fields including the IS field. The central theme of the SET is rationality (Blau, 1964). The SET defines social exchange as the exchange of tangible or intangible activities between parties based on the trade-offs of rewards and costs. The parties involved in the exchange have no contractual obligations. Instead, the parties expect reciprocal benefits while calculating the costs they have to pay for the exchange (Blau,

  ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

1964; Homans, 1958). According to the SET, in marketplaces, consumers make using vs. not using, buying vs. not buying, or adopting vs. not adopting decisions based on the trade-offs of rewards and costs (Blau, 1964; Homans, 1958). In IS field, the SET has been applied to studies in different exchange contexts. Nicolaou and McKnight (2011) applied the SET in the context of repeated electronic data exchange between organizations and found that increased perceived information quality as an exchange reward had increased data exchange intention. Turel et al. (2010) examined the impact of the perceived exchange values on consumers' adoption of hedonic digital artifacts. However, past research has disproportionally focused on the impacts of rewards when adopting the SET, while cost perceptions such as privacy and security concerns may play a deterrent role in consumers' decisions on e-commerce in general and m-commerce in particular. Thus in this study, we adopted the SET to develop an integrated model in which both users' perceptions of exchange rewards and costs in m-commerce are examined.

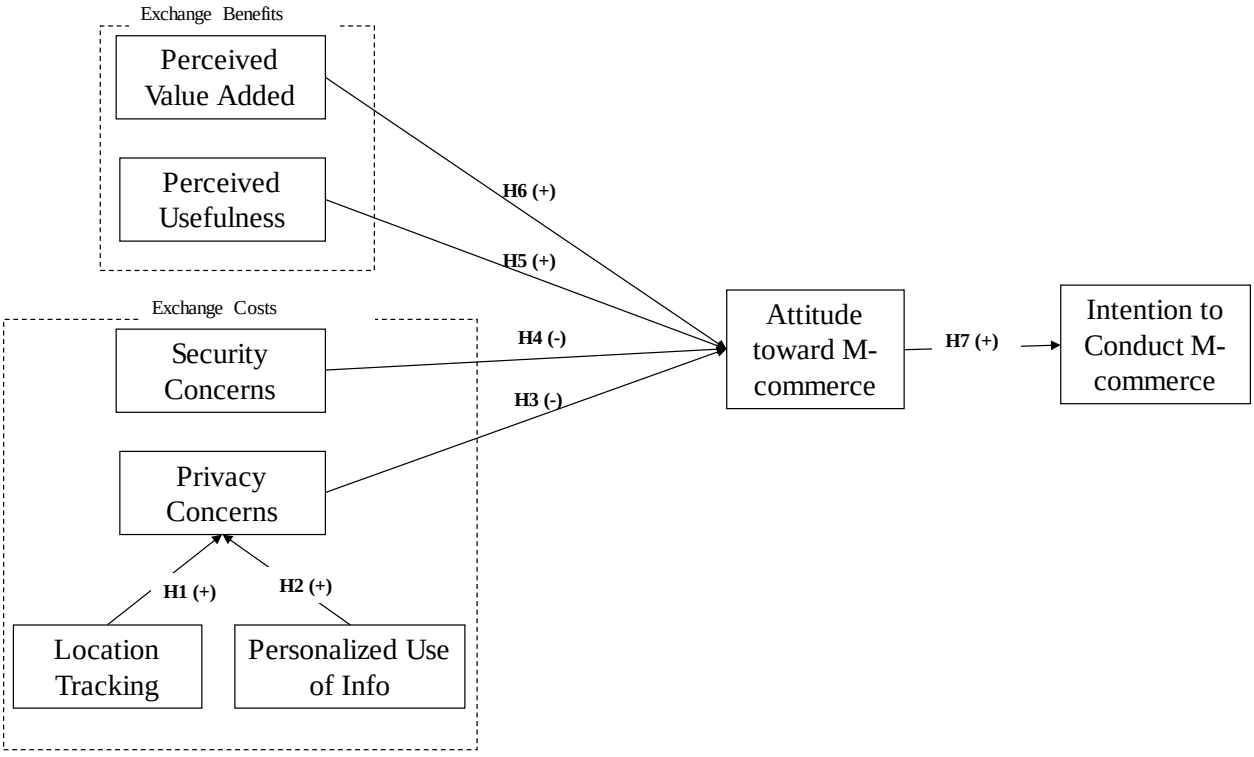
RESEARCH MODEL AND HYPOTHESIS DEVELOPMENT

Drawing upon the SET (Blau, 1964; Homans, 1958), we developed the following research model as shown in Figure 1. We argued that due to the nature of mobile computing technology as discussed in Section 1, users make their decision on whether or not conducting m-commerce based on the trade-offs of rewards and costs. In the context of m-commerce, the two major cost concerns are privacy concerns and security concerns, and perceived value added and perceived usefulness are two major reward perceptions, as suggested by literature (Dai et al., 2010; Siau et al., 2001; Turel et al., 2010). We further argued that users' cost and rewards perceptions impact their m-commerce attitude which in turn impacts their intention to conduct m-commerce according to the theory of reasoned action (TRA) (Fishbein & Ajzen, 1975). The proposed research model examines users' "calculus"-like decision process that includes both privacy and security concerns as well as perceived exchange benefits (Dinev et al., 2013). Moreover, the model takes the situational privacy concerns into consideration. The proposed research model serves as the theoretical foundation for the following hypothesis development.

Mobile computing can attach a person's identifier to the personal information that has been collected. As a result, companies can utilize such information at micro, individual level in addition to macro, aggregated level (Earp et al., 2005). Personalized use of personal information is defined as using users' personal information such as personal preferences and past behavioral patterns to provide tailored products and product purchasing experiences with or without users' consent (Chellappa & Sin, 2005). When Amazon greets a returning user with the name or when a mobile app recommends a product based on the user's previous transaction with another e-vendor, the user may ask: How do they know that? Past research has pointed out that personalized use of personal information was an inhibiting factor in e-commerce and caused privacy concerns among consumers (Chellappa & Sin, 2005). Past research also found that although personalization provides benefits and convenience to users, the cost of it is the privacy concerns (Awad & Krishnan, 2006). Based on above rationale, we propose the following hypothesis:

H2. Personalized use of personal information positively impacts users' privacy concerns in m-commerce.

Figure 1: Research Model.



As we discussed before, privacy concerns refer to individuals' worry about collection, use and error of information collected from them (Smith et al., 1996). In the information age, keeping the information regarding one's self private is an ethical, legal, and practical challenge (Smith et al., 1996). IS studies have intensively examined the inhibiting impact of privacy concerns on various attitudes and intentions in various contexts. Past research has found that privacy concerns on the use of Internet for online shopping influenced the formation of favorable attitudes toward online shopping (Salisbury et al., 2001). In the context of adopting electronic health records systems, privacy concerns were found to change patients' attitudes toward electronic health records systems (Angst and Agarwal, 2009). Thus we argue that users' privacy concerns will negatively impact their favorable attitudes toward m-commerce.

H3. Users' privacy concerns negatively impact their attitudes toward conducting m-commerce.

Security breaches can put users' personal and financial information in a great danger. Consequently, users may suffer identify theft and financial loss later on. Target's credit card security breach in the Christmas shopping season in 2013 has stirred up great security concerns on all e-business platforms, either wired or wireless. As a result, Target's sale took a big hit (ABC News, 2014). This indicates that security concerns can significantly change consumers' favorable attitudes toward the business (Chen & Dai, 2014). In other words, security concerns can paralyze consumers and thus fundamentally change their attitudes and beliefs (Chellappa, 2002; SAP, 2013). IS research has long recognized the relationship between users' security concerns and their

attitudes toward e-commerce (Furnell & Karweni, 1999). Following the above logic, we thus hypothesize:

H4. Users' security concerns negatively impact their attitudes toward conducting m-commerce.

The SET indicates that it is rational that consumers choose and buy what they feel worth of it. Consumers would engage in a relationship with a product/service or the company behind it because of the rewards perceived by them (Zeithaml, 1988). Unlike economic exchange, social exchange emphasizes intangible, subjective benefits from the perspective of human perception (Blau, 1964; Homans, 1958). Thus the SET posits that in a social exchange, people attempt to maximize their rewards and minimize their costs in order to purse the largest net reward (Blau, 1964; Homans, 1958). Past IS research has long recognized that perceived usefulness is a key subjective benefit perceived by users in adopting an IS technology (Davis et al., 1989). Perceived usefulness is defined as the possible performance improvement perceived by users when adopting a technology and is a major determinant of various technology acceptance attitudes and behaviors in various contexts including in the context of m-commerce (e.g. Lu et al., 2003). Thus we hypothesize:

H5. Users' perceived usefulness positively impact their attitudes toward conducting m-commerce.

Mobile devices provide mobility and convenience to users. With mobile devices, users can access the Internet and conduct m-commerce anytime and anyplace at will, thus providing additional benefits to users (Lu et al., 2003). Since perceived value added is obtained from the user' interaction and experience with m-commerce, it includes a set of values in the context of m-commerce, such as timely access to information and immediate purchase opportunity. Past IS research (e.g. Nicolaou & McKnight, 2011; Turel et al., 2010) has found that users' perceived value in various social exchange situations changed their attitudes and intention of exchange. Thus we argue that added value perceived by users will positively impact their favorable attitudes to m-commerce.

H6. Users' perceived value added positively impacts their attitudes toward conducting m-commerce.

In this study, intention to conduct m-commerce is a proxy of actual behaviors. According to the TRA (Fishbein & Ajzen, 1975), intention is a consequent of attitude. A person's attitude indicates the person's favorable or unfavorable evaluations and action tendencies toward actual action (Fishbein & Ajzen, 1975). Numerous studies (e.g. Tsang et al., 2004) have confirmed the link from attitude to behavioral intention. Thus we argue that users' favorable attitudes to m-commerce will result in increased intentions to adopt m-commerce. We also argue that m-commerce encompasses many more activities including mobile shopping, mobile banking, and mobile social communication. Based on the above rationale, we thus hypothesize,

H7. Users' attitudes toward conducting m-commerce positively impact their intentions to conduct m-commerce.

  ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

RESEARCH METHOD

This study applied survey methodology to empirically test the research model and hypotheses. A survey instrument was developed based on an extensive literature review to ensure the content validity of the instrument. The development of the instrument was also based on the guidelines suggested by IS literature (e.g. Straub et al., 2004). Most measurement items were adopted from existing measures and adapted to fit the current context of the study.

A 7-point Likert scale ranging from 'strongly disagree' to 'strongly agree' was used for each item in the instrument except for those demographic items. The items used to measure consumers' privacy concerns were adapted from Smith et al. (1996) and Stewart and Segars (2002). The items for two situational privacy concern constructs, location tracking and personalized use of personal information, were adapted from Kaasinen (2003) and Earp et al. (2005) respectively. The items for security concerns were adapted from Chellappa (2002). The items to measure perceived usefulness were adapted from Davis et al. (1989) and the items to measure perceived value added were adapted from Siau et al. (2001). The items for attitudes to m-commerce were adapted from Bagozzi et al. (1992). Finally, the items to measure intention to conduct m-commerce were based on the literature and developed by this study. All measurement items were reflective and multi-item scales were used to ensure the reliability and validity of the measurement. Demographic items were also added in the survey questionnaire.

The back translation method was used to develop the Chinese version of the survey questionnaire. An English version of the questionnaire was first developed based on our research model and an extensive literature review. The survey instrument was pilot tested on several experienced m-commerce users who were also familiar with the topic of the research. The questionnaire was refined based on the feedback from the pilot test. The questionnaire was then translated into Chinese and tested on several Chinese users. Afterwards, a bilingual researcher translated the questionnaire back to English to ensure the accuracy and consistency of the Chinese translation. Minor modification on the Chinese questionnaire was made according to the back translation. The Chinese questionnaire was used to solicit the survey participants' opinions on the focal constructs of the research.

The survey was randomly distributed by one of the researchers in a metropolitan area in China where m-commerce had been well advocated by local companies and the government. M-commerce was also relatively well diffused among the city population. 200 survey questionnaires were distributed to students of a university, employees of a commercial organization and employees of a government agency, who reported having used mobile devices for at least three months. The participants spent about 20 minutes to complete the survey. Among 200 questionnaires distributed, 141 were responded. The survey response rate was 70.5%. Six questionnaires with most survey questions unanswered were subsequently dropped, resulting in a total of 135 usable responses in the data sample for the subsequent data analysis.

Demographic statistics of the participants show that there was a good distribution of age in our sample. 31.1% of the participants were above 35 years old, 32.6% were in the age group of 26-35, and 36.3% were in the age group of 18-25. All participants had the experience of using mobile devices. 66.7% of them had used mobile devices for more than four years. In terms of the gender

  ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

distribution of the sample, 57% of the participants were male and 43% were female, indicating a reasonable even distribution of gender in the sample.

DATA ANALYSIS

In the data analysis, we used partial least squares (PLS) method to test the measurement model and the structural model. PLS is a suitable statistical technique for our study since it is a component-based approach and places minimal restrictions on measurement scales, sample size, and residual distributions (Chin et al., 2003). We first tested the validity of the instruments. The reliability of the constructs is established when Cronbach's α values are greater than 0.70, average variance extracted (AVE) values are greater than 0.5, and composite factor reliability (CFR) values are above 0.5 (Gefen & Straub, 2005; Straub et al., 2004; Segars, 1997). As shown in Table 1, the Cronbach's α values ranged from 0.79 to 0.93, the AVEs were between 0.50 to 0.79, and CFR values were all above 0.70. Thus, the reliability of the constructs was validated. We also validated the convergent and discriminant validity of the constructs. All items were loaded to the construct as the items were intended to and all loadings were greater than 0.70. No cross-loadings on the constructs were greater than 0.4, which confirmed the convergent validity (Gefen & Straub, 2005; Straub et al., 2004). The discriminant validity is established (1) when the square root of AVE for each construct is greater than its correlations with other constructs and (2) when the loadings of items on the intended construct are greater than the loadings on other constructs (Gefen & Straub, 2005; Straub et al., 2004). The square root of each AVE shown on the diagonal of the inter-construct correlation matrix in Table 1 was greater than the correlations underneath it, demonstrating the discriminant validity. The factor analysis results also demonstrate that the criteria were satisfied, establishing the discriminant validity of the constructs.

Table 1: Inter-Correlation Matric and Reliability Checks.

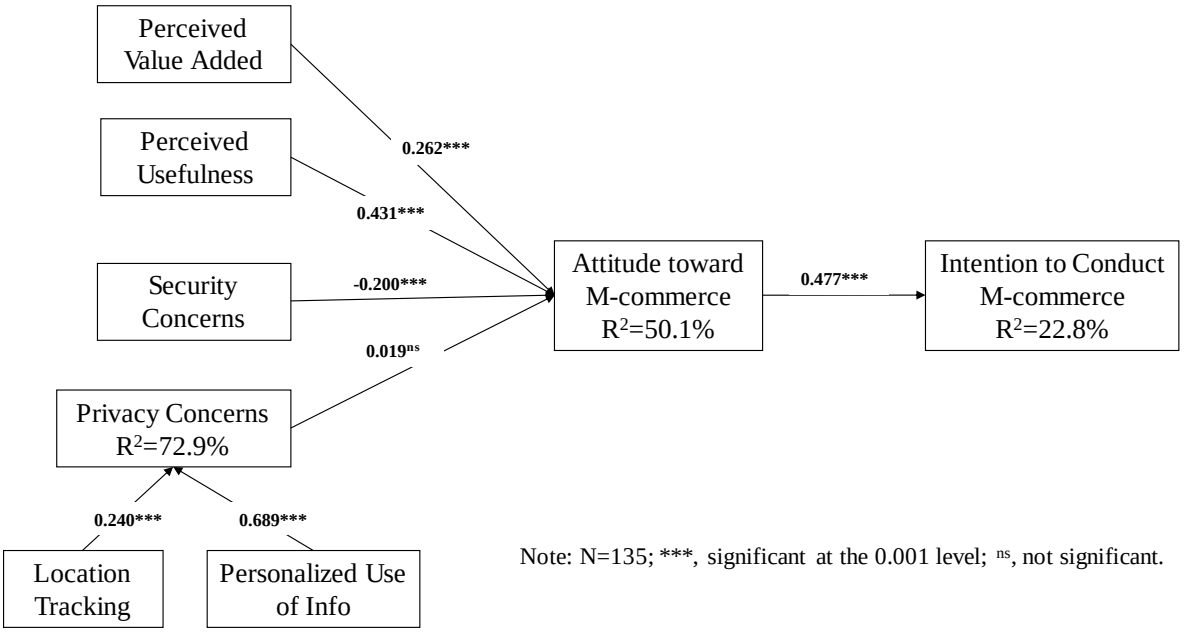
	Inter-Construct Correlation matrix								AVE	CFR	Cronbach's α
	1	2	3	4	5	6	7	8			
1. Attitude	**0.84**								0.71	0.88	0.79
2. Intention	0.48	**0.85**							0.72	0.93	0.90
3. Location tracking	0.16	0.17	**0.89**						0.79	0.92	0.87
4. Perceived usefulness	0.64	0.43	0.17	**0.87**					0.76	0.94	0.92
5. Perceived values added	0.61	0.42	0.14	0.64	**0.85**				0.72	0.91	0.87
6. Personalized use of info	0.13	0.21	0.59	0.13	0.14	**0.89**			0.78	0.95	0.93
7. Privacy concerns	0.18	0.20	0.83	0.17	0.17	0.65	**0.86**		0.74	0.92	0.88
8. Security concerns	-0.37	-0.22	-0.19	-0.26	-0.26	-0.26	-0.19	**0.76**	0.57	0.87	0.82

Note: Bold font values on the diagonal of the correlation matrix are the square root values of AVEs.

Using the bootstrapping resampling procedure in PLS, we estimated the structural model. Figure 2 summarized the results of the model estimation including the path coefficients and their significant levels based on the p-values as well as the explained variances. Of the seven hypotheses we proposed six were statistically significant at the 0.001 level. As shown in Figure 2, users' reward perceptions in terms of perceived usefulness and perceived value added had a significant impact on users' favorable attitude toward m-commerce with the path coefficients of 0.431 and

0.262 respectively (H5 and H6). As hypothesized, there was a strong, negative association between users' security concerns and their positive attitude toward m-commerce with a path coefficient of -0.200 (H4). Moreover, the link between users' privacy concerns and location tracking was significant with a path coefficient of 0.240 (H1). The association between users' privacy concerns and personalized use of personal information was supported too with a strong path coefficient of 0.689 (H2). Location tracking and personalized use of personal information together explained 72.9% of the variance in privacy concerns. The results also supported that users' favorable attitude toward m-commerce had a significant effect on their intention to conduct m-commerce with a path coefficient of 0.477 (H8). The two perceived exchange benefit constructs and two perceived exchange cost constructs together explained 50.1% of the variance in attitude toward m-commerce which in turn explained 22.8% of variance in intention to conduct m-commerce. Interestingly, H3, hypothesizing the association between users' privacy concerns and their attitudes toward m-commerce, was not supported by our results.

Figure 2: Model Estimation.



Note: N=135; ***, significant at the 0.001 level; ns, not significant.

DISCUSSION AND CONCLUSION

Drawing upon the social exchange theory (SET), we developed the research model in which users' perceptions on the exchange benefits and costs in m-commerce and the consequent effects of such perceptions on users' attitudes toward m-commerce were examined. In addition, the research also integrated both privacy concerns and security concerns in the research model while accounting for the effects of situational privacy concerns specific to the context of m-commerce. Users' value perceptions specific to the context of m-commerce were also accounted in the research model. Using the survey approach, we collected 135 observations from the survey participants in a large city in China. Our data analysis results supported all the hypotheses except for H3, thus confirming our conceptualization of the research model.

In detail, our findings related to two users' perceived exchange benefits constructs, perceived value added and perceived usefulness, are in general consistent with the SET and some findings in IS literature. The significant paths linking from perceived value added and perceived usefulness to m-commerce attitude indicate that to promote users' favorable attitudes toward m-commerce, we need to provide users with additional functional and non-functional benefits in m-commerce. This could help managers develop value-based strategies to strengthen customers' attitude toward m-commerce which could benefit business survival and marketing extension. The findings also pointed out that performance and convenience of m-commerce are the determinants in increasing users' favorable attitudes toward m-commerce.

Our findings further pointed out that users' security concerns are a deterrent factor in their attitude toward m-commerce, confirming the SET in which perceptions on social exchange costs have hindering effects on the exchange (Blau, 1964; Homans, 1958). Our findings are also consistent with some findings in IS research. For example, security concerns have been found to paralyze users and thus they tend to take less proactive security countermeasures while withdrawing from beneficial online activities such as online shopping and banking (Chen & Zahedi, 2009). Therefore, while there is a need to continuously seek various technical security solutions and architectures in mobile computing, studying users' security perceptions and alleviating their security concerns are also critical in prompting m-commerce.

Furthermore, the associations between the two situational privacy concerns, location tracking and personalized use of personal information, and general privacy concerns were strong. The findings are in accordance with the theoretical model in this study and indicate that users may feel very uncomfortable and concerned when e-vendors tie the collected information directly to a user with his/her identifier. In other words, aggressively utilizing personalization and location tracking may backfire on m-commerce.

Interestingly, our findings regarding the relationship between users' privacy concerns and their attitude toward m-commerce are not consistent with some findings in IS literature (e.g. Salisbury et al., 2001). A possible explanation is that more and more users have realized that their personal information is almost constantly collected by various parties on the Internet, no matter via wired or wireless connection. The mobile platform enables various parties collect more specific information such as current location from users. However, it is almost impossible for today's users to give up mobile devices such as smart phones as well as benefits and convenience brought by such devices just because of the additional information collected from them. Our findings indeed indicate that in certain circumstances, users would not dramatically change their attitude toward a specific technology and may continuously use the technology, even though they are concerned about their privacy. A recent study by Yun et al. (2013) pointed out that there is a risk shift phenomenon in which users demonstrated risk-taking behaviors to continually use LBS even when they expressed strong privacy concerns. Our findings indeed indicated that users may take risks of possible privacy violation in exchange for functional and non-functional benefits of m-commerce. Another plausible explanation is that Chinese culture is a collectivist culture in which people are more cooperative and obedient. Under the influence of collectivist culture, users are more willing to give up some degree of individual privacy to exchange for benefits in social exchanges (Johnston et al., 2009). Thus privacy concerns may be less of a matter in m-commerce among Chinese users. Our findings also interestingly pointed out that security concerns have a more

  ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

substantial inhabiting effect on m-commerce diffusion than privacy concerns. It seems that when facing the privacy vs. use paradox, users may relinquish certain degree of their privacy. However, this is not the case when it comes to security.

Our research has both theoretical and practical implications. Theoretically, this research advances our understanding of m-commerce behavior by empirically validating the proposed research model in which influencing factors of m-commerce use comprise a set of beliefs in exchange benefits and costs. Moreover, our model provides insight into users' complex decision-making process in m-commerce and the relative strength of the inhibitors and the drivers in m-commerce. The theoretical model based on the SET can also advance our understanding of the antecedents of behavioral intention in m-commerce by going beyond factors in technology acceptance model and its variants. Another significant implication of this study is that unlike many other studies on privacy concerns in the IS field, our study integrates both privacy and security concerns into the research model. In particular, this study sheds light on some interesting directions for studying information privacy and security: (1) there might be a risky shift phenomenon in which users might relinquish their privacy concerns to certain extent in exchange for benefits in m-commerce use and (2) security concerns might be a stronger inhibitor than privacy concerns in m-commerce.

This study is also important for practitioners in m-commerce. To conduct m-commerce, practitioners must exercise clear policies that state how the information is used and protected to alleviate users' privacy and security concerns. On the other hand, practitioners in m-commerce should focus more on functional and non-functional benefits of their mobile products and services, since perceptions on values and usefulness are the key drives in m-commerce. Managers should strive to design services free of cost for use, because with the cost considerations, customers' benefit expectations may be diminished, which will in turn ruin their benefit assessment and attitude to continue using m-commerce.

Furthermore, the current study may serve as a theoretical benchmark for practitioners in m-commerce to evaluate their quality and functionality of the m-commerce products/services and the effectiveness of their practice on informing privacy and security.

Another practical implication is that this study informs businesses seeking to enter Chinese mobile markets of specific information about Chinese users' privacy and security concerns, attitudes and intentions in m-commerce. Our research findings provide guidance to businesses on how to deliver targeted campaigns and specific m-commerce products/services in Chinese markets. Our findings regarding a possible risky shift phenomenon among Chinese users are particularly revealing. Businesses may be able to provide more customized m-commerce products/services to build long-term trust and relationship with Chinese users by utilizing collected personal information. This also points out an interesting further research topic: Does privacy have a price? If it does, what is the price the user would accept in order to voluntarily provide his/her information for target marketing?

As other studies, our study has its limitations which might be addressed in future studies. The sample size might be a limitation. We collected our data in a single city in China. Although we tried to reach a broad population by sending the survey to difference organizations, the sample is still a convenient sample with a relatively small sample size. In addition, the data was collected in

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

merely a single metropolitan cultural environment in China. It does not represent all cultural environments such as rural cultural environments and not represent the complete population of m-commerce users in China. While the cultural homogeneity in survey participation is appropriate when the research goal is to develop and test theories, cautions should be taken when generalizing our findings in different cultural environments and populations. Thus a future research direction might be a duplication of this study to a larger population with cultural diversity. In addition, common method bias (CMB) might be a limitation of this study since we collection the data via a cross-sectional fashion though certain precautions were taken to remedy this issue when developing the survey. A future longitudinal study might mitigate this limitation.

REFERENCES

ABC News. (2014). Target (TGT) Profits hit by card security hack. Available at: http://abcnews.go.com/Business/target-profits-hit-card-security-hack/story?id=22680841 (last accessed on February 28, 2104).

Angst, C. M., & Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: the elaboration likelihood model and individual persuasion. *MIS Quarterly*, 33(2), 339-370.

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly*, 30(1), 13-28.

Bagozzi, R., Baumgartner, H., & Yi, Y. (1992). State vs. action orientation and the theory of reasoned action. *Journal of Consumer Research*, 18(4), 505-518.

Blau, P. (1964), *Exchange and Power in Social Life*, Wiley, New York, NY.

Chellappa, R.K. (2002). Consumers' trust in electronic commerce transactions: the role of perceived privacy and perceived security. Working paper, Goizueta Business School, Emory University Atlanta, GA, USA.

Chen, Y., & Dai, H. (2014). Do Innovators Concern Less about Security and Value New Technologies More? A Case of Mobile Commerce. Journal of Information Technology Management, 25(4), 13-26.

Chen, Y. & Zahedi, M. (2009). Internet users' security behaviors and trust. In *Proceeding of the Fourth AIS SIGSEC Workshop on Information Security & Privacy*, December 15-16, Phoenix, Arizona.

Chin, W.W., Marcolin, B. L., & Newsted, P. R. (2003).A partial least squares latent variable modeling approach for measuring interaction effects: results from a Monte Carlo simulation study and an electronic mail emotion/adoption study. *Information Systems Research*, 14(2), 189-217.

ChinaInternetWatch (2014). China Mobile Shopping Market Snapshot in 2013. Available at: http://www.chinainternetwatch.com/6025/china-mobile-shopping-market-2013/ (Last accessed on February 26, 2104).

Dai, H., Wen, K-W., Singh, R., & Iyer, L.S. (2012). An integrative framework of mobile commerce consumers' privacy concerns and willingness to use: an empirical study. *International Journal of Electronic Business*, 10(1), 79-100.

Davis, F.D., Bagozzi, R.P., & Warshaw, P.R. (1989). User acceptance of computer technology: a comparison of two theoretical models. *Management Science*, 35(8), 982-1003.

Dinev, T., Xu, H, Smith, J. H., & Hart, P. (2013). Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, 22(3), 295-316.

Dutta, A., & McCrohan, K. (2002). Management's role in information security in a cyber economy. *California Management Review*, 45(1), 67-87.

Earp, J.B., Anton, A.I., Aiman-Smith, L., & Stufflebeam, W.H. (2005). Examining internet privacy policies within the context of user privacy values. *IEEE Transactions on Engineering Management*, 52(2), 227-237.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research reading*. Addison-Wesley Publishing Company.

Flavián, C. & Guinalíu, M. (2006). Consumer trust, perceived security and privacy policy: Three basic elements of loyalty to a web site. *Industrial Management + Data Systems*, 106(5), 601-620.

Forrester, (2011). Mobile Commerce Forecast: 2011 To 2016. Available at: http://www.forrester.com/Mobile+Commerce+Forecast+2011+To+2016/fulltext/-/E-RES58616?objectid=RES58616 (Last accessed on February 18, 2104).

Furnell, S.M. & Karweni, T. (1999). Security implications of electronic commerce: a survey of consumers and businesses. *Internet Research*, 9(5), 372- 382.

Gartner, (2013). Gartner Says Worldwide PC, Tablet and Mobile Phone Shipments to Grow 4.5 Percent in 2013 as Lower-Priced Devices Drive Growth. Available at: http://www.gartner.com/newsroom/id/2610015 (Last accessed on February 18, 2104).

Gauzente, C. (2004). Web merchants' privacy and security statements: how reassuring are they for consumers? a two-sided approach. *Journal of Electronic Commerce Research*, 5(3), 191-198.

Gefen, D., Straub, D. W., & Boudreau, M.-C. (2000). Structural equation modeling and regression: guidelines for research practice. *Communications of the Association for Information Systems*, 4, 1-79.

Ghosh, A.K. and Swaminatha, T.M. (2001). Software security and privacy risk in mobile e-commerce. *Communications of the ACM*, 44(2), 51-57.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organizations. *European Journal of Information Systems*, 18(2), 106-125.

Homans, G. C. (1958). Social behavior as exchange. *American Journal of Sociology*, 63(6), 31-41.

Johnston, A. C., Warkentin, M., & Luo, X. (2009). National culture and information privacy: the influential effects of individualism and collectivism on privacy concerns and organizational commitment. In: *Proceedings of the International Federation for Information Processing (IFIP) International Workshop on Information Security Research*, Cape Town, South Africa.

Kaasinen, E. (2003). User needs for location-aware mobile services. *Personal and Ubiquitous Computing*, 7(1), 70-79.

Li, H., Sarathy, R., & Xu, H. (2010). Understanding situational online information disclosure as a privacy calculus. *Journal of Computer Information Systems*, 51(1), 62-71.

Lindell, M. K., & Whitney, D. J. (2001). Accounting for common method variance in cross-sectional research designs. *Journal of Applied Psychology*, 86(1), 114-121.

Lu, J., Liu, C., Yu, C., & Yao, J. (2003). Acceptance of wireless internet via mobile technology in China. In : *Proceedings of Ninth Americas Conference on Information Systems*, August 4-6,Tampa, FL, USA.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): the construct, the scale and a causal model. *Information Systems Research*, 15(4), 336-355.

Nicolaou, A. I., & McKnight, D. H. (2011). System design features and repeated use of electronic data exchanges. *Journal of Management Information Systems*, 28(2), 269-304.

Podsakoff, P. M., & Organ, D. W. (1986). Self-reports in organizational research: Problems and prospects. *Journal of Management*, 12(4), 531-544.

Salisbury, W. D., Pearson, R. A., Pearson, A. W., & Miller, D. W. (2001). Perceived security and World Wide Web purchase intention. *Industrial Management + Data Systems*, 101(4), 165-177.

SAP, (2013). The mobile consumer insights on global trends impacting mobile momentum and customer engagement. Available at:

http://www.sap.com/pc/tech/mobile/featured/offers/mobile-consumer-behaivor-report.html. (Last accessed February 18, 2104).

Segars, A. H. (1997). Assessing the unidimensionality of measurement: a paradigm and illustration within the context of information systems research. *Omega*, 25(1), 107-121.

Siau, K., Lim, E. P., & Shen, Z. (2001). Mobile commerce: Promises, challenges and research agenda. *Journal of Database Management*, 12(3), 4-13.

Siau, K., Sheng, H., Nah, F., & David, S. (2004). A qualitative investigation on consumer trust in mobile commerce. *International Journal of Electronic Business*, 2(3), 283-300.

Smith, J. H., Milberg, S. J., & Burke, S. J. (1996). Information privacy: measuring individuals' concerns about corporate practices. *MIS Quarterly*, 20(2), 167-196.

Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research*, 13(1), 36-49.

Straub, D., Boudreau, M-C, & Gefen, D. (2004). Validation guidelines for is positivist research. *Communications of the AIS*, 13, 380-426.

Tsang, M. M., Ho, S.-C., & Liang, T.-P. (2004). Consumer attitudes toward mobile advertising: An empirical study. *International Journal of Electronic Commerce*, 8(3), 65-78.

Turel, O., Serenko, A., & Bontis, B. (2010). User acceptance of hedonic digital artifacts: A theory of consumption values perspective. *Information & Management*, 47(1), 53-59.

Van Slyke, C., 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.

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.

Yun, H., Han D., & Lee, C. C. (2013). Understanding the use of location-based service applications: Do privacy concerns matter? *Journal of Electronic Commerce Research*, 14(3), 251-230.

Zeithaml, V. A. (1988). Consumer perceptions of price, quality and value: a mean-end model and synthesis of evidence. *Journal of Marketing*, 52(3), 2-22.

  ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy