Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2007 Proceedings

Americas Conference on Information Systems (AMCIS)

December 2007

An Investigation of Consumer's Security and Privacy Perceptions in Mobile Commerce

Hua Dai
University of North Carolina at Greensboro

Lakshmi Iyer
The University of North Carolina at Greensboro

Rahul Singh
University of North Carolina, Greensboro

An Investigation of Consumer's Security and Privacy Perceptions in Mobile Commerce

Abstract

This study investigates the composition of consumer's security and privacy perceptions of mobile commerce (m-commerce) and the factors shaping these security and privacy perceptions. Based on literature review, we examined the effect of eight determinants: information type, information collection, secondary use of information, error, unauthorized access, location awareness, information transfer, and personalization; on security and privacy concerns in the m-commerce context. Analysis of data from 141 respondents revealed three dimensions for the security and privacy perception construct. Hence, three models were tested to address the impacts of these factors on the three dimensions: consumers' confidence of information control, concerns on third party, and the awareness of information protection in the m-commerce context. The study has implications for professionals to meet the consumers' requirements and expectations on security and privacy for m-commerce.

Keywords: Privacy, Security, Mobile Commerce, Information Collection, Location Awareness, Personalization, Unauthorized access, Secondary Use.

Introduction

Information privacy and security concerns have shown to be a major obstacle in the development of consumer-related electronic commerce (e-commerce) (Miyazaki and Fernandez, 2001; Earp and Anton, 2004). People's perceptions of information privacy and security concerns have important influence on their intention to participate in or conduct e-commerce activities (Malhotra et al, 2004; Brown and Muchira, 2004; Sah and Han, 2003). By the turn of the new century, consumer's activities have started to shift from "E-decade" to "M-decade" (Wagner, 2005). The advancements in mobile technology and telecommunication infrastructure have stimulated the growth in use of mobile services which previously was accomplished through traditional methods or use of the Internet.

The GSM (global system for mobile communications) cell phone system and the Internet have been viewed as one of two dominant global communication networks. Currently there are about 1.02 billion Internet users[1], while the GSM has over 2 billion customers in 210 countries and territories (Wikipedia). According to the consultants McKinsey & Company, by 2010, mobile commerce (m-commerce) will be the second-largest industry in the world (Rao, 2001).

With tremendous potential for growth in mobile industry, there has been notable increase in studies on adoption, penetration and usage of mobile devices and services in recent research (Siau and Shen, 2003; Jarvenppa and Lang, 2005; Harris et al, 2005). However, from the practical perspective, the development of m-commerce has been comparatively slow (Mylonakis, 2004). Some barriers have been found in recent studies including uncertain technology standards, complexities of interactive multimedia application, the threat of government regulation, user interface, pricing structure, and security and privacy risks which are contributing to a deflated vision of m-commerce (Jarvenppa et al. 2003; Reid, 2001; Ghosh and Swaminatha, 2001). Those barriers force researchers and practitioners to consider deep level of reasoning for the low acceptance rate of m-commerce.

Mobile devices combine communication and computing capabilities with mobility and personality (Jarvenppa and Lang, 2005). Thus, the user's own perception is very important in adopting mobile technologies. Jarvenpaa and Todd (1997) indicate the need to research the relationship between perceived characteristics of Web shopping and user intentions. Similar studies in the m-commerce context will help organizations develop appropriate strategies to promote m-commerce. Contrast to e-commerce which relies on wired Internet, m-commerce relies on wireless Internet and is exposed to greater danger of insecurity since hackers may intercept anywhere in the free air (Lu et al, 2003). Therefore, gaining customer trust in m-commerce is a particularly daunting task because of its unique features (Siau and Shen, 2003). Thus, there are new security and privacy risks particular to use of mobile devices that can dampen consumer adoption of mobile services (Ghosh and Swaminatha, 2001). Without understanding the user's perception, the mobile vendor cannot provide corresponding service and technology features to meet the customers' requirements which would lead to loss of consumer's trust and low rate of adoption.

[1] http://www.internetworldstats.com/stats.htm

With huge potential for growth in m-commerce, understanding the security and privacy concerns of consumers is critical. The purpose of the study is to investigate what factors affect the security and privacy perception in the m-commerce context? We also investigate, based on prior literature, the dimensionality of security and privacy perceptions in m-commerce. The next section covers the literature review. We then present our initial hypotheses, research methodology, analysis of results and implications. We finally summarize with limitations and directions for further research.

Literature Review

Security and Privacy

The issues of privacy and security have been labeled by government and consumer organizations as two major concerns of e-commerce (EC) (CNN 2000; Customer Reports Online; Miyazaki and Fernandez, 2001). The privacy of consumer information that is collected for commercial purposes is seen as a distinct consumer right from both legal and ethical perspectives. In addition, the secure storage and transmission of consumer information is seen as an integral step in maintaining that privacy (Miyazaki and Fernandez, 2001.) Besides, the growing body of consumer-oriented internet research that is focusing on privacy and security related issues (Milne, 2002) suggests that these issues may play a significant role in developing online retailing (Miyazaki and Fernandez, 2001).

The main purpose of this paper is to address the consumers' security and privacy perceptions in m-commerce. Before we define the perceptions of security and privacy, we should first get a clear understanding of the concepts of security and privacy. Security refers to 'the policies, procedures, and technical measures used to prevent unauthorized access, alteration, theft, or physical damage' (Laudon and Laudon, 2003). Warren and Brandeis (1890) define privacy as "the right of an individual to be let alone", which is the definition that many authors still recognize (Stahl, 2004). Dutta and Macrohan (2002) distinguished the concept of privacy and security. They indicated that "privacy" deals with the degree of control that and entity, whether a person or organization, has over information about itself, while the "security" deals with vulnerability to unauthorized access to content.

Both concepts are very important and has been discussed in the IS literature. In the m-commerce context, Gosh and Swaminatha (2001) indicate that in spite of the seemingly unlimited potential to drive new applications and markets in mobile e-commerce, new security and privacy risks particular to the wireless medium and devices abound in m-commerce applications. Lu et al (2003) point out that wireless security must be seen in the broader context of Internet-based e-commerce systems to include confidentiality, authentication, and message integrity. To build consumer's trust in the safety of using wireless devices for transaction, wireless transport layer security (WTLS), public key infrastructure (PKI), certificate authority (CA), Wired Equivalent Privacy (WEP), device independent smart card, and wireless biometric services have emerged as common solutions (Kay 2002). However, there has been little published research regarding the perceptions of security and privacy, particularly in the m-commerce context.

Security and Privacy Perceptions

Perceptions about using the World Wide Web for purchasing products will lead to the formation of attitudes that will influence intent to purchase products on the World Wide Web (Salisbury et al, 2001). Therefore, getting an understanding of the characteristics of customers' perceptions of m-commerce is critical to mobile business vendors. This research mainly deals with the perceptions of security and privacy among those characteristics. Prior studies have investigated perceptions of security and privacy in the context of trust and risks in e-commerce. For example, Chellappa (2001) proposed that the guarantee of integrity on every aspect of EC transaction will be as expected to be determined by the consumers' perception of risk to their privacy and security of information. Thus, the overall trust in EC transaction is a consumer's subjective evaluation of both the entity's characteristics (Beccera and Gupta, 1999) and risk created by security and privacy perceptions. In the mobile context, this subjective evaluation still exists. People expect security protection and demand that their privacy be not intruded when they use mobile devices for m-commerce activities.

In terms of conceptualization of security and privacy perceptions, some prior literature defined these two perceptions in different context. Salisbury et al (2001) define perceived web security as the extent to which one believes that the World Wide Web is secure for transmitting sensitive information. With regards to security concerns of online consumers, consumer perceptions of unsatisfactory security on the Internet continue to exist even when vendors undertake security enforcement mechanisms (Miyazaki and Fernandez, 2001; Zellweger, 1997). Udo (2001) indicates that security concern is one of the main reasons users do not purchase over the Web. Consumer reluctance to Internet commerce is partly due to the fact that the barrier to shopping on the Internet is relatively high. In the mobile context, failing to provide a secure system of m-commerce will significantly dampen consumer adoption rates (Ghosh and Swaminatha, 2001).

Smith, et al. (1996) identified four factors: collection, errors, secondary use and unauthorized access as the dimensions of an individual's concern for privacy and developed a Concern for Information Privacy (CFIP) instrument. Later research has argued that "CFIP needs to reinvestigate in light of emerging technology, practice and research," (Stewart and Segars, 2002). Websites usually require personal information from the users for the purposes such as membership, newsletter subscription, feedback forms, order forms, etc. Consumers have worried for years about how personal data is used by government and more recently, by business (Udo, 2001). In the mobile environment, since the openness adds more risks, people would have higher demand of privacy protection. So, providing consumers with information about how their personal data are used and exploring the possibilities of offering consumers privacy preference are among the issues to be addressed (Rubin, 1995).

Two problems have been identified in the EC literature regarding the conceptualization of consumers' security and privacy perceptions. They include the extent to which privacy and security perceptions are defined as distinct concepts and the lack of understanding of how they are related. It is unknown whether consumers really see these as distinct issues (Belanger et al, 2002). Two possible views have been adopted in previous studies. First, Perceived security and perceived privacy are treated as two distinct concepts (Chellappa, 2001; Belanger et al., 2002). For example, Chellappa (2001) indicate that perceived privacy and perceived security are indeed distinct constructs but there is a need to consider the possibility of mediated effect on trust in EC. A second view is to treat these two perceptions as a whole concept or use global terms to represent both privacy and security concerns. Jones (1991) point out that even if privacy and security of a transaction are enforced through distinct principles, it is possible that consumers may perceive security and privacy to be somewhat related concepts. In investigating the years of experience's impacts on people's security and privacy concerns, Miyazaki and Fernandez (2001) show that consumer's perceptions of security and privacy risks of their transactions as being somewhat equivalent. Dutta and MacCrohan (2002) address that one cannot achieve privacy without appropriate security mechanisms. Therefore, in this study we use the security and privacy perceptions as a global term and identify the components under this total perception.

Conceptual Framework

Information Collection

The growing collection of personal information has been a theme in privacy literature sine the 1970s. The collection construct was described by Smith et al (1996) as the concern that extensive amounts of personally identifiable data are being collected and stored in databases. Based on the framework they developed for concern for information privacy instrument, they indicated that collection is one of four important determinants of people's perception of privacy. Later, Stewart and Segars (2002) did an empirical examination of the concern for Information privacy instrument with which they proved the collection is a valid construct to measure people's privacy concern.

Information Types

Beckwith (2003) define the information sensitivity as a function of what information is shared. In another words, different types of information would influence people's perception of security and privacy. Chellappa (2002) pointed out that the information collected online broadly falls into three categories: (1) anonymous information, typically the standard information sent with any Web or Internet request; (2) personally non-identifying information, such as age, date of birth, gender, occupation, education, income, ZIP Code with no address, interest and hobbies; and (3) personally identifying information that refers to information that can be used to identify or locate an individual. The cumulative effect of these information types can be more telling on the privacy of the consumer as information across categories can be combined, allowing for use of information in ways that were not feasible or practical before (Culnan and Armstrong, 1999).

Secondary Use of Information

Sometimes information is collected from individuals for one purpose but is used for another, a secondary purpose without authorization from the individuals (Smith et al, 1996). This concern was raised pointedly in the code of Fair Information Practices, which was included in a seminal study sponsored by the US department of health, education, and welfare (1973). Although questionable security is a major deterrent to online shopping, concerns regarding the secondary use of information loom large, discouraging consumers from engaging in online relationship exchanges (Hoffman et al 1999). Control over secondary use of information is likely to be a sticking point.

Errors

The dimension of errors has been defined by Smith et al (1996) as a concern that protections against deliberate and accidental errors in personal data are inadequate. Many individuals believe that organizations are not taking enough steps to minimize problems from errors in personal data. Although some errors might be deliberate, most private-related concerns involve instead accidental errors in personal data (Smith et al, 1996). Stewart and Segars (2002)'s study empirically tests and confirms the significant effects of error dimension on individual Concern for Information Privacy. It was indicated that the error dimension addresses the question of whether or not companies are taking the steps and formulating the policies to minimize inappropriate access to data as well as errors in personal data.

Unauthorized Access

The unauthorized access concern means that data about individuals are readily available to people not properly authorized to view or work with this data (Smith et al, 1996). Smith indicated that although technological options now exist for controlling such access at file, record, or field level, how those options are utilized and how polices associated with those uses are formed represent value-laden management judgment. It tells that companies should take more steps to make sure that unauthorized people cannot access personal information in their computers.

Location Awareness

A mobile phone can be located by the telecom operator in the network. Privacy protection in location-aware services is related to the right to locate a person, use the location, store the location and forward the location (Kaasinen, 2003). Some recent studies (Hong and Landay, 2004; Minch's 2004) have addressed the relation between customer's privacy concern and location based services in m-commerce. Developers, retailers, and consumers need to be on the same page in understanding how their personal information is used especially with the newly-developed location information that can be tied directly to these highly personal data. In Kaasineen's (2003) study, people were worried about their privacy and the "big brother" phenomenon when considering services enabling people to be located.

Information transfer

Privacy in information transfer means the insurance that other cannot find something out during any transfer of information. This addresses the transfer of information as well as to whom the information is transferred (Earp et al, 2005). In Earp et al' study, the survey results showed that users are most concerned with the information transfer that their data will be shared, lent, or sold to other entities.

Personalization

Chellappa and Sin (2005) defined personalization as the ability to proactively tailor products and product purchasing experiences to tastes of individual consumers based upon their personal and preference information. They identified two critical factors related personalization in consumers' online shopping: vendors' ability to acquire and process consumer information, and consumers' willingness to share information and use personalization services. It was pointed out that investments in online personalization may be severely undermined if consumers do not use these services due to privacy concerns, so it is of critical importance that vendors understand and evaluate the different values consumers may place in enjoying various types of personalization Chellappa and Sin (2005).

On the basis of theoretical foundations described above, we developed the following research model and initial hypothesis (table 1) to investigate the factors that shape security and privacy perceptions in m-commerce:

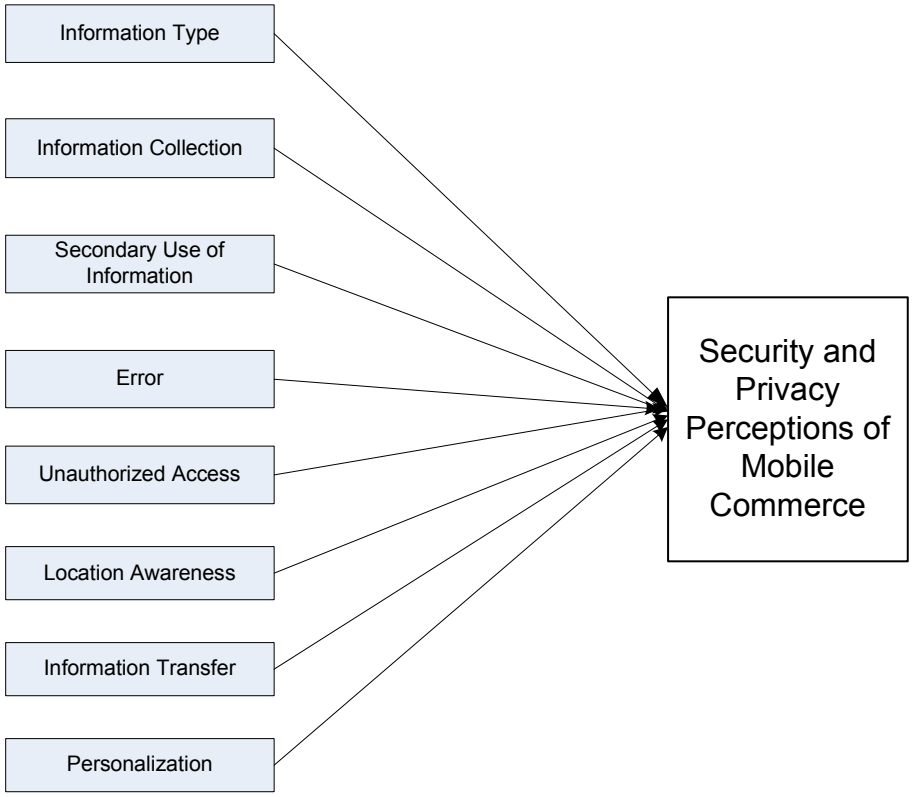

Figure 1: Proposed Research Model

Table 1: Initial Hypotheses

H1: There is a positive association between information type and consumer's security and privacy perceptions of m-commerce
H2: There is a positive association between information collection and consumer's security and privacy perceptions of m-commerce
H3: There is a positive association between secondary use of information and consumer's security and privacy perceptions of m-commerce
H4: There is a positive association between error consumer's security and privacy perceptions of m-commerce
H5: There is a positive association between unauthorized access and consumer's security and privacy perceptions of m-commerce
H6: There is a positive association between location awareness and consumer's security and privacy perceptions of m-commerce
H7: There is a positive association between information transfer and consumer's security and privacy perceptions of m-commerce
H8: There is a positive association between error and consumer's security and privacy perceptions of m-commerce

Research Method

The purpose of this study is to understand consumer's perceptions of security and privacy of m-commerce. Different perceptions as reported in this paper were identified by reviewing the literature. To empirically test our model, a survey instrument was developed based on prior research as discussed in the next sub-section.

An English version of the questionnaire was first developed based on the research model and exhaustive literature review. The survey instrument was pilot tested on several experienced m-commerce users who are also familiar with research issues

on privacy and security concerns. The aim of the pilot survey was to test the feasibility of the instrument and gain qualitative feedback from the respondents. Based on this feedback, changes were made to improve the layout of the survey form and the phrasing of some survey questions. Later, the questionnaire was translated into Chinese-Mainland version. The revised survey, in Chinese, was distributed in one of the big cities in China where m-commerce is largely diffused and promoted by vendors. 200 questionnaires were distributed, out of which 141 responses were collected. Respondents included students, employees of a company and a government organization. This generated a 70.5% response rate. Six incomplete questionnaires were dropped later in data analysis due to the inadequate information provided yielding 135 useable responses.

Measures

The purpose of each of the items on the survey instrument was to give the consumers the opportunity to express their opinions and views concerning their perception of security and privacy regarding m-commerce. The items were simple statements of concerns for which the participants were asked to indicate their opinions on a scale of `strongly disagree to strongly agree'.

Independent Variables

The items used to measure *information collection, secondary use of information, errors, and unauthorized access* were replicated from Smith et al (1996) *and* Stewart and Segars', (2002) studies on Concern for Information Privacy – CFIP. Smith et al (1996) developed and validated the instrument of the CFIP which identifies and measures the primary dimensions of individuals' concerns about organizational information privacy practices. Later, Stewart and Segars (2002) conducted an empirical examination to test all the items identified in Smith's research. Their results suggest that each dimension of this instrument is reliable and distinct. Total 15 items were developed to address the four dimensions of Concern for Information Privacy. We applied all these fifteen items in our study on people's security and privacy perceptions in m-commerce. All items were measured with a seven-item seven-point Likert-type scale (1 = "Strongly disagree" to 7 = "Strongly agree"). The data demonstrated that Cronbach's Alpha measure of 0.9367 for information collection is 0.9101; second use of information 0.9619; error 0.8849; and the unauthorized access 0.8819.

Other measures were generated from literature review on security and privacy perceptions and key word searches of security perception, privacy perception, perceived security, perceived privacy, security concerns, privacy concerns, risks, and m-commerce. There are also some measures from MIS survey instrument in the AIS world website. A total of 13 items were generated to identify different types of information could be collected for m-commerce services. These items represent the degree to which of the various information that people are willing to share in m-commerce. The Cronbach's alpha for this scale is .0.9512. Personalization and Information transfer were measured by the items developed in Earp et al (2005) study on examining internet privacy policies within the context of user privacy values. Five scales and three scales are applied to measure the personalization and Information transfer in terms of people's security and privacy perceptions in m-commerce activities. The Cronbach's alpha value for personalization is 0.9307 and for information transfer is 0.9051. Location awareness was measured with a three-item seven-point Likert-type scale. These three scales developed for this study were based on the research of Minch (2004) and Kaasinen (2003)'s study. The Cronbach's alpha is 0.8711 for this scale.

Dependent Variable

The security and privacy perception is treated as a global concept in our study. 13 items were used to measure the consumers' perceptions of security and privacy. These items were developed in Chellappa (2001)'s study on security and privacy perceptions in e-commerce transactions. Out of the 13 items, 7 items were defined for perceived privacy and 6 items for perceived security based on discriminate validities in ecommerce environment. The items for privacy perceptions measure how a consumer believes her information is handled in response to claims and other technological investments for privacy protection employed by online sellers and the security perceptions as relates to organizational user's concern of security that is measured through user assessment of security effectiveness (Goodhue and Straub, 1991).

Exploratory Factor Analysis

We factor analyzed the 135 usable records. Those items that loaded less than 0.40 or cross-loaded were discarded. This analysis resulted in eight factors viewed as our independent variables: *Information Type, Information Collection, Secondary Use of Information, Error, Unauthorized Access, Location Awareness, Information Transfer,* and *Personalization*. Table 2 shows the descriptive statistics and the correlations matrix of these factors:

Table 2: Descriptive Statistics and Correlations

	Mean	Std. Deviation	N	IT	IC	SUI	E	UA	LA	ITR	P
IT	4.3284	1.58733	135	1							
IC	4.9160	1.56216	135	.653	1						
SUI	5.7130	1.64859	135	.527	.732	1					
E	5.2864	1.36478	135	.344	.485	.573	1				
UA	5.4037	1.39450	135	.368	.546	.685	.923	1			
LA	5.5210	1.39435	135	.534	.675	.776	.633	.722	1		
ITR	5.6185	1.54679	135	.406	.582	.724	.576	.679	.702	1	
P	5.1878	1.55213	135	.373	.514	.587	.531	.592	.592	.703	1

The loadings for the dependent variable security and privacy perception were not grouped together as expected. The factor analysis resulted in 3 groups of items. These loadings are displayed in table 3:

Table 3: Factor Matrix for Security and Privacy Perceptions

	Factor		
	1	2	3
SP1	.537		
SP2	.776		
SP3	.823		
SP4	.791		
SP5	.702		
SP6R			.394
SP10R			.714
SP12R			.783
SP7		.555	
SP8		.668	
SP9		.614	
SP11		.635	
SP13		.672	

Therefore, we divided the security and privacy perceptions into three categories based on the loadings of the items and their descriptions. The first category is labeled as Confidence of Information Control (CIC). This category has also been discussed in some prior work (Malhotra et al, 2004; Phelps et al., 2000). Malhotra et al (2004) emphasized that control is especially important in the information privacy context because consumers take high risks in the submission of personal information. The second category is defined as the Concerns about Third Parties (CTP). This category address the concerns that people have regarding a sharing information for any other purposes with third parties. The third one is named as Awareness of Information Protection (AIP). Awareness is a passive dimension of information privacy, and it refers to the degree to which a consumer is concerned about his/her awareness of organizational information privacy practices (Culnan 1995; Foxman and Kilcoyne 1993). These awarenesses are captured through such CFIP factors as unauthorized secondary use, improper access, and errors (Malhotra et al, 2004). Accordingly, we re-formulate the hypotheses with respect to the proposed research model (Table 4):

Table 4: Revised Hypotheses

H1a. There is a positive association between information type and mobile consumer's confidence of information control. *H1b. There is a positive association between information type and consumers' concerns on third party in mobile commerce.* *H1c. There is a positive association between Information type and mobile consumer's awareness of information protection.*
H2a. There is a positive association between information collection and mobile consumer's confidence of information control. *H2b. There is a positive association between information collection and consumers' concerns on third party in mobile commerce.* *H2c. There is a positive association between Information collection and mobile consumer's awareness of information protection.*
H3a. There is a positive association between secondary use of information and mobile consumer's confidence of information control. *H3b. There is a positive association between secondary use of information and consumers' concerns on third party in mobile commerce.* *H3c. There is a positive association between secondary use of information and mobile consumer's awareness of information protection.*
H4a. There is a positive association between error and mobile consumer's confidence of information control. *H4b. There is a positive association between error and consumers' concerns on third party in mobile commerce.* *H4c. There is a positive association between error and mobile consumer's awareness of information protection.*
H5a. There is a positive association between unauthorized access and mobile consumer's confidence of information control. *H5b. There is a positive association between unauthorized access and consumers' concerns on third party in mobile commerce.* *H5c. There is a positive association between unauthorized access and mobile consumer's awareness of information protection.*
H6a. There is a positive association between location awareness and mobile consumer's confidence of information control. *H6b. There is a positive association between location awareness and consumers' concerns on third party in mobile commerce.* *H6c. There is a positive association between location awareness and mobile consumer's awareness of information protection.*
H7a. There is a positive association between information transfer and mobile consumer's confidence of information control. *H7b. There is a positive association between information transfer and consumers' concerns on third party in mobile commerce.* *H7c. There is a positive association between information transfer and mobile consumer's awareness of information protection.*
H8a. There is a positive association between error and mobile consumer's confidence of information control. *H8b. There is a positive association between error and consumers' concerns on third party in mobile commerce.* *H8c. There is a positive association between error and mobile consumer's awareness of information protection.*

All constructs were subject to a reliability test and the results are shown in Table 5. Chronbach's alpha for all constructs are above 0.70.

Table 5: The Results of Reliability Test

Construct	Cronbach's α
Information Type	0.9512
Information Collection	0.9101
Second Use of Information	0.9619
Error	0.8849
Unauthorized Access	0.8819
Location Awareness	0.8711
Information Transfer	0.9051
Personalization	0.9307
Confidence of Information Control	0.8743
Concerns on third party	0.7016
Awareness of information protection	0.8158

Hypotheses Results and Discussions

The three models were subject to simple regression tests. The standard coefficients and the significance level are depicted in the figures below:

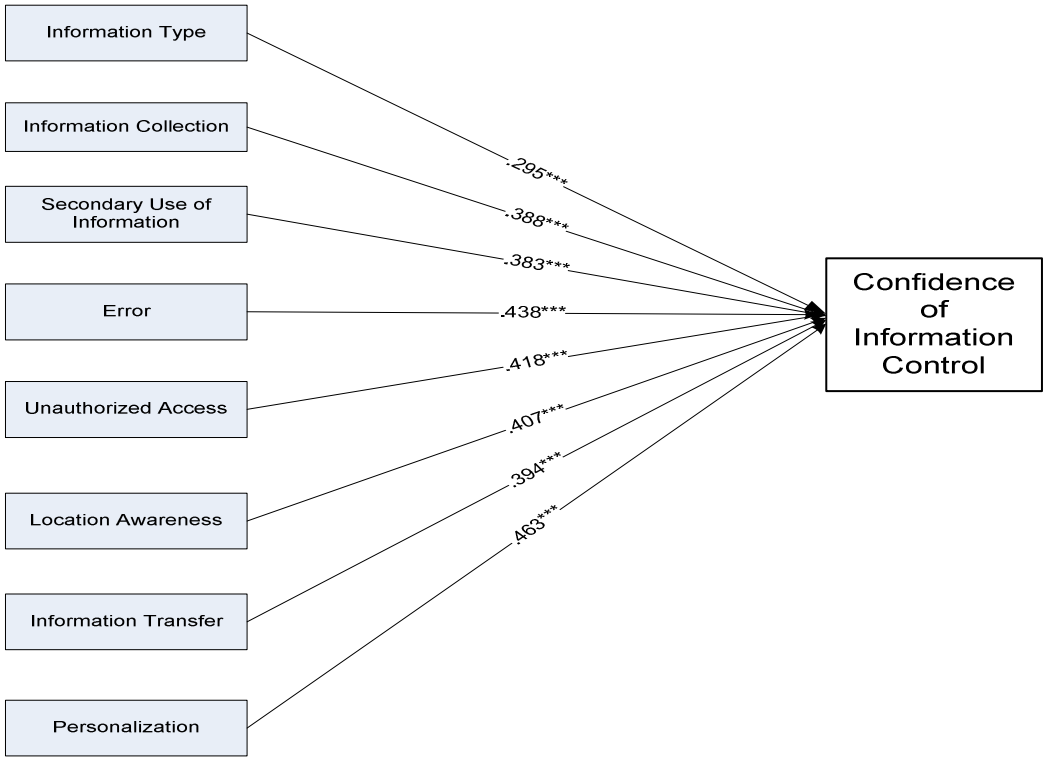

Figure2: Factors Affecting Confidence of Information Control in M-commerce
Significance Level: *** for <0.001, **<0.01, *<0.05

The results indicate that Hypotheses 1a, 2a, 3a, 4a, 5a, 6a, 7a, 8a are all supported by data. The regression of each factor on the confidence of information control is significant with p-value less than 0.001. Thus, we can concluded that *Information Type, Information Collection, Secondary Use of Information, Error, Unauthorized Access, Location Awareness, Information Transfer*, and *Personalization* shape consumers confidence of information control in their m-commerce activities.

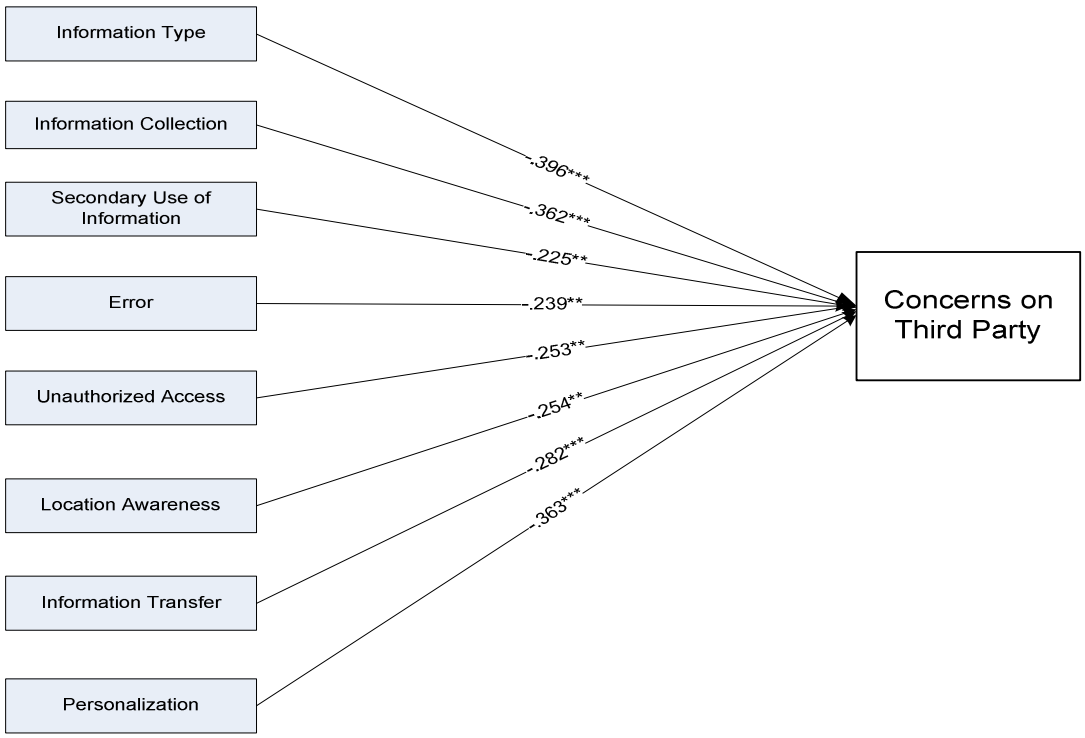

Figure 3: Factors Affecting Concerns on Third Party in M-commerce
Significance Level: *** for <0.001, **<0.01, *<0.05

Similarly, the Hypothesis1b, 2b, 3b, 4b, 5b, 6b, 7b, and 8b are all supported by data. The regression results show that *information type*, *information collection*, *information transfer*, *and personalization* have a significant impact on consumers' concerns on third party with p-value less than 0.001. The *secondary use of information*, *error*, *unauthorized access*, and *the location awareness* are also associated with consumers' concerns on third party in m-commerce with significant p-value less than 0.01 in our tests.

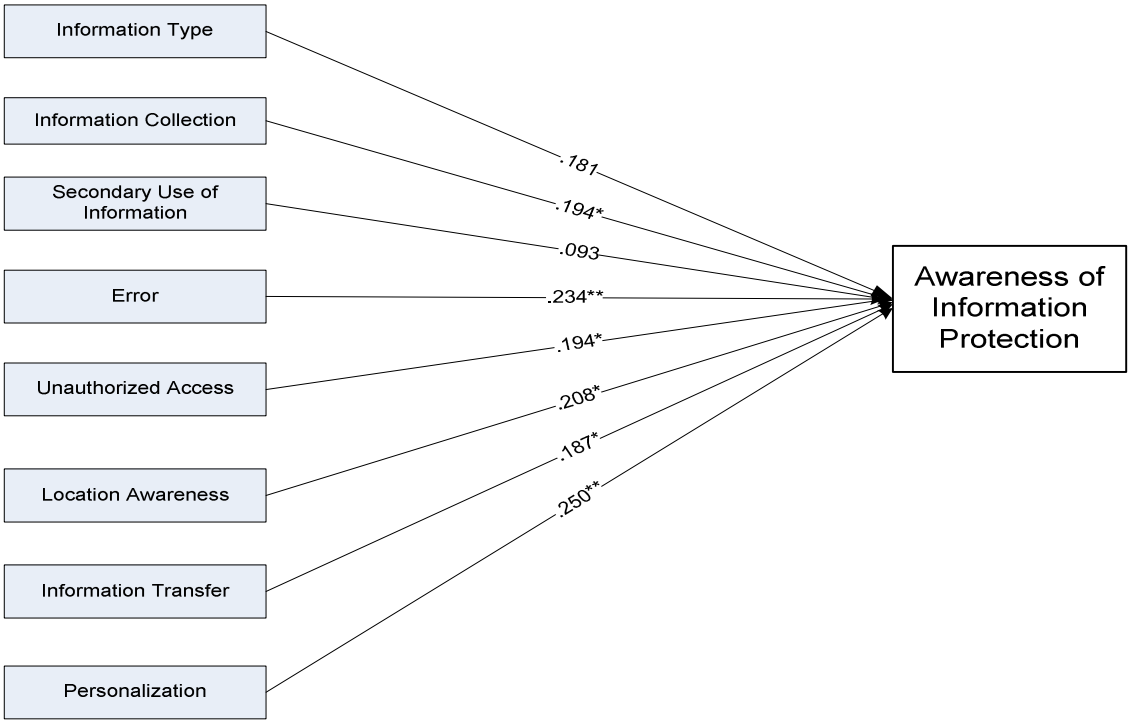

Figure 4: Factors Affecting Confidence on Information Protection in M-commerce
Significance Level: *** for <0.001, **<0.01, *<0.05

In the third sub-set model, the *information type* factor does not influence consumers' awareness of information protection in m-commerce. The explanation might be that Chinese consumers don't care if different protection methods are in place for different types of information. *Secondary use of information* was also found to not have a significant impact on consumers' awareness of information protection in m-commerce. One explanation could be that if consumers are aware of secondary use, they would not expect any protection of their privacy and security. So, other than H1c and H3c, Hypothesis 2c, 4c, 5c, 6c, 7c, and 8c are all supported by our data. Therefore, the factors *Information Collection*, *Error*, *Unauthorized Access*, *Location Awareness*, *Information Transfer*, and *Personalization* are all determinants of consumers' awareness of information protection in m-commerce. Table 6 shows a summary of the hypotheses tests.

Table 6: Summary of Hypotheses tests

Hypothesis	p-value			Hypothesis test
H1a	0.001			Supported
H1b		0.000		Supported
H1c			0.181	Not supported
H2a	0.000			Supported
H2b		0.000		Supported
H2c			0.024	Supported
H3a	0.000			Supported
H3b		0.009		Supported
H3c			0.282	Not Supported
H4a	0.000			Supported
H4b		0.005		Supported
H4c			0.006	Supported
H5a	0.000			Supported
H5b		0.003		Supported
H5c			0.024	Supported
H6a	0.000			Supported
H6b		0.003		Supported
H6c			0.016	Supported
H7a	0.000			Supported
H7b		0.001		Supported
H7c			0.030	Supported
H8a	0.000			Supported
H8b		0.000		Supported
H8c			0.003	Supported

Implications

Although various technical security solutions and architectures exist within the scope of IT and mobile technology such as cryptography, digital signatures, certificates, and authentication, consumers still have security and privacy concerns. Understanding consumers' security and privacy perceptions is significant to promote m-commerce growth. This study provides valuable insights for mobile vendors and IT security and privacy professionals to understand consumers' perception of security and privacy issues in using m-commerce.

The current security and privacy practice in m-commerce activities are not aligned with the security and privacy practices users want to see. This study serves as an initial step toward proactive security and privacy practice management by mobile business vendors and other professionals can adopt to instill better privacy and security policies. To meet the users' requirement and expectations on security and privacy of m-commerce transactions an important task is to build consumers' trust of m-commerce, and correspondingly improve low adoption rates of m-commerce. Since the mobile service providers have to be more vocal in promoting the security features that are available to users when they interact online with mobile device, when the users become more aware of the security functions and believe that their privacy will not be intruded, then they would be willing to use m-commerce.

The study contributes to the academic audience by identifying factors affecting security and privacy concerns in m-commerce. In addition, we show that the security and perceptions are not necessarily a one-dimensional construct. Further research on some of the consequents of these dimensions will help determine causal relationships between security and privacy concerns and adoption issues in m-commerce.

Summary

This study investigates the composition of consumer's security and privacy perceptions of m-commerce and the factors shaping these security and privacy perceptions of consumers. The effect of eight determinants: information type; information collection; secondary use of information; error; unauthorized access; location awareness; information transfer; and personalization were studied. Analysis of the security and privacy perceptions yielded three constructs: consumers' confidence in information control, concerns about third parties, and awareness of information protection. Three models were tested to address the impacts of these factors on the above three dependent constructs. The results demonstrate that all these factors play important role in shaping consumers confidence in information control and concerns about third parties. The two factors not affecting awareness of information protection were information type and secondary use of information. This is important for practitioners as they must exercise clear policies that state how the information is used and protected. This will help alleviate consumers' concerns about m-commerce security and privacy.

The validity of our results strongly depends on the sampling of the surveyed subjects. All the respondents are from the same city in China. While differences in ethnicity exist it may be homogeneous in nature and life style. Replicating the study in several cities in China would help in generalizing the results. A similar study in different countries might yield interesting results based on cultural differences. Another possible direction for future research is to look at consequents of security and privacy concerns in m-commerce.

References

1. Beccera, M. and Gupta, A.K. "Trust within the Organization: Integrating the Trust Literature with Agency Theory and Transaction Cost Economics," *Public Administration Quarterly*, 1999, 177-203.

2. Belanger, F., Hiller, J. S., and Smith, W. J., "Trustworthiness in electronic commerce: The role of privacy, security, and site attributes," *Journal of Strategic Information Systems*, 11, 2002, 245–270,

3. Brown, M. and Muchira, R., "Investigating the Relationship between Internet Privacy Concerns and Online Purchase Behavior," *Journal of Electronic Commerce Research*, (5:1), 2004

4. Chellappa, R. K. and Sin, R., "Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma," *Information Technology and Management*, (6:2-3), 2005

5. Chellappa, R.K., " Consumers' Trust in Electronic Commerce Transactions: The Role of Perceived Privacy and Perceived Security," under submission

6. CNN. 200. Survey: Most in U.S. Want Companies to Guarantee Online Privacy. Cahle News Network online, August 21, available online at http://www.cnn.com/2000/TECH/computing/08/18/privacy.report/index.html

7. Culnan, M. J. "Consumer awareness of name removal procedures: Implications for direct marketing," J. *Direct Marketing* (9:2), 1995, 10–19.

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

9. Customer Reports Online, 1998. Some Bits and Bytes of Consumer-Friendly sites, http://www.consumersunion.org/special/samples/reports/98/12shp2.htm, accessed by Miyazaki, A.D., Fernandez at 1998

10. Dutta, A. and McCrohan, K., "Management's Role in Information Security in a Cyber Economy," *California Management Review*, (45:1), 2002,67-87

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

12. Earp, J.B. and Anton, A.I., "Addressing End-User Privacy Concerns", *Proceedings of the Tenth Americas Conference on Information Systems*, New York, 2004

13. Foxman, E. R., and Kilcoyne, P. "Information technology, marketing practice, and consumer privacy: Ethical issues," *Journal of Public Policy Marketing* (12:1), 1993, 106–119

14. Ghosh, A. K. and Swaminatha, T. M., "Software Security and Privacy Risk in Mobile E-commerce," *Communications of the ACM*, (44:2), 2001.

15. Goodhue, D.L. and Straub, D.W. "Security Concerns of Systems Users: A Study of Perceptions of the Adequacy of Security," *Information and Management* (20), 1991, 13-27.

16. Harris P., Rettie R. and Kwan C. C. "Adoption and Usage of M-Commerce: A Cross-Cultural Comparison of Hong Kong and United Kingdom," *Journal of Electronic Commerce Research*, (6:3), 2005

17. Hoffman, D.L., Novak, T.P., Peralta, M., "Building consumer trust online". *Communications of the ACM* (42:4), 1999, 80–85

18. Hong, J.I. and Landay, J.A. "Architecture for privacy-sensitive ubiquitous computing," *Proceedings of 2nd International Conference on Mobile Systems, Applications, and Services (MobiSys)*, Boston , 2004

19. Jarvenpaa S.L. and Lang K.R. "Managing the paradoxes of mobile technology", *Information Systems Management* (22:4), 2005, 7-23

20. Jarvenpaa, S.L. and Todd, P.A., "Consumer reactions to electronic shopping on the world wide web", *International Journal of Electronic Commerce*, (2:1), 1997

21. Jarvenpaa, S.L., Lang, K.R. and Takeda, Y.; Tuunainen, V.K. "Mobile Commerce at Crossroad," *Communications of the ACM*. (46:2), 2003, 41-44.

22. Jones, M.G. "Privacy: A significant marketing issue for the 1990s," *Journal of public Policy and Marketing* (10), 1991, 133-148.

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

24. Kay, R. "Wireless Security," *Computer World*, (36:26), 2002, 38-39.

25. Laudon, K; Laudon, J., Essentials of Management Information Systems Fifth Edition. Prentice Hall: New Jersey, 2003

26. Lu, J. Liu, C. Yu, C. and Yao, J., "Acceptance of Wireless Internet via Mobile Technology in China," *Proceedings of Ninth Americas Conference on Information Systems*, 2003

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

28. Milne, G. R., "Privacy and Ethical Issues in Database/Interactive Marketing and Public Policy: A Research Framework and Overview of the Special Issue." *Journal of Public Policy & Marketing*, 19, spring 2000, 1-6.

29. Minch, R. P., "Privacy issues in location-aware mobile devices," *In Proceedings of the 37th Hawaii International Conference on System Sciences*, 5–8 January 2004, Big Island, Hawaii

30. Miyazaki, A.D.and Fernandez, A., "Consumer perceptions of privacy and security risks for online shopping", *The Journal of Consumer Affairs*, (35:1) 27-44. 2001

31. Mylonakis, J., "Can Mobile Services Facilitate Commerce? Findings from the Greek Telecommunications Market", *International Journal of Mobile Communication*, (2:2) 188-198, 2004

32. Phelps, J., Nowak, G. and Ferrell, F. "Privacy concerns and consumer willingness to provide personal information," *Journal Public Policy Marketing* (19:1), 2004, 27–41.

33. Beckwith. R, "Designing for ubiquity: The perception of privacy," *Pervasive Computing*, (2:2) April-June 2003, 40–46

34. Rao, M. "South Korea Aims for Global Leadership in Wireless, Broadband Internet Markets in Information Age," (available online at http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan006689.pdf), Accessed March 28, 2006.

35. Reid, H. M., 2001, "Remarks to security and privacy for government online" Available at URL: http://infocom.gc.ca/speeches/speechview-e.asp?intspeechId=5

36. Rubin, M. R., "Private Rights, Public Wrongs: The Computer and Personal Privacy", John Wiley and Sons: New York, 1995.

37. Salisbury, W.D., Pearson, R.A., Pearson, A.W. and Miller, D.W., "Perceived security and world wide web purchase intention", Industrial Management & Data Systems, (101:4), 2001, 165-76.

38. Siau, K. and Shen, Z., "Building customer trust in mobile commerce", *Communications of ACM*, (46:4), April 2003, 91–94.

39. Smith, J.H., Milberg, S.J. and Burke, S.J. "Information Privacy: Measuring Individuals' Concerns About Corporate Practices," *MIS Quarterly* (20:2), 1996, pp. 167-196.

40. Stahl, B. (2004) "Responsibility for Information Assurance and Privacy: A Problem of Individual Ethics?," *Journal of Organizational and End User Computing*, (16:3), 59-77.

41. Stewart, K.A. and Segars, A.H. "An Empirical Examination of the Concern for Information Privacy Instrument," *Information Systems Research* (13:1), 2002, pp. 36-49

42. Suh, B., Han, I., "The impact of consumer trust and perception of security control on the acceptance of electronic commerce", *International Journal of Electronic Commerce,* (7:3), 2003, pp, 135-161,

43. Udo, G.J.,'Privacy and Security Concerns as Major Barriers for E-commerce: A Survey Study', *Information Management & Computer Security*, (9:4), 2001, pp. 165- 174

44. Wagner, M.J., "Cutting the cords", *The American City & County*, (120:13), Dec 2005, pg-38.

45. Warren, S. and L., Brandeis (1890) "The Right to Privacy," *Harvard Law Review*, (4:5), 193-220

46. www.wikipedia.org

47. Zellweger, P. "Web-based sales: Defining the cognitive buyer," *Electronic Markets* (7:3), 1997, pp. 10-16.