

# The Influence of Intention to Use the Mobile Banking - The Privacy Mechanism Perspective

Juo-Tzu Tseng

Department of Information Management

National Central University, Jhongli, 32001 Taoyuan, Taiwan

Tel: 886-03-422-7151(66500) E-mail: ruorose@gmail.com

Hsiang-Lin Han

Department of Information Management

National Central University, Jhongli, 32001 Taoyuan, Taiwan

Tel: 886-03-422-7151(66500) E-mail: sgps2004200297@gmail.com

Yea-Huey Su

Department of Information Management

National Central University, Jhongli, 32001 Taoyuan, Taiwan

Tel: 886-03-422-7151(66500) E-mail: suesu101@gmail.com

Yi-Wen Fan

Department of Information Management

National Central University, Jhongli, 32001 Taoyuan, Taiwan

Tel: 886-03-422-7151(66500) E-mail: iwfangary@gmail.com

Received: Nov. 2, 2016 Accepted: Dec. 30, 2016 Published: January 10, 2017

doi:10.5296/jmr.v9i1.10580

URL: <http://dx.doi.org/10.5296/jmr.v9i1.10580>

---

**Abstract**

With the rapid development in digital and mobile technologies, banks or other financial institutions have provided various mobile banking solutions or services to their customers for enabling mobile commerce. However, there is always a trade-off between convenience and security for people to decide whether they adopt mobile banking services or not. In the mobile age, people are concerned for transaction security and information privacy immensely. Accordingly, how to provide the secured financial services to their customers become more important for a bank. Survey research method is imported to understand how the privacy mechanism, including privacy policy and privacy empowerment, influences the adaption of mobile banking. Based on a survey of 425 participants, we used a structural equation modeling approach to investigate the research model. The results indicate that privacy mechanisms are matter for people to concern about the privacy of their personal information and their intention to use mobile banking. In other words, we found that privacy empowerment is significant which in turn led customers to be more likely to adopt mobile banking.

**Keywords:** Mobile Banking, Privacy Mechanism, Concerns for Information Privacy, Social Contract Theory

## 1. Introduction

The convergence of the Internet, wireless technologies and mobile devices has led to mobile commerce (m-commerce) a new paradigm of an emerging information technology (Luo, Li, Zhang, and Shim, 2010). Therefore, financial institutions deliver online services via various electronic channels subsequently diminishing the importance of conventional branch networks (Chan, 2013). In today's commerce, mobile banking has gained significant importance, and the growth of the field is accelerating (Lin, 2011; Afshan and Sharif, 2016). Market Intelligence & Consulting Institute (MIC) (2015a) presented emerging information issues of banking. They focused on digital innovation applications and payments including digital banking application, mobile payment, and third-party payment. Zhou, Lu, and Wang (2010) proposed technology characteristics that are critical aspects of mobile banking technology including ubiquity, immediacy, and security. Mobile banking users break through the limit of space and time. Mobile Banking is a salient system (Turban, King, Viehland, and Lee, 2006). According **the survey on broadband Internet usage in Taiwan** in 2016, mobile networking drives a new life-style; 26% use mobile banking, and 21.8% use mobile payment (Taiwan Network Information Center [TWNIC], 2016). The data show that while the amount of mobile device users continues to increase, few use mobile banking and payments. This will extend from financial transactions to the electronic or physical shopping realm as well as ordering and logistics. It is effective in enhancing the convenience of the life-style of the user.

Security and privacy are critical in e-services such as Internet banking (Hanafizadeh, Keating, and Khedmatgozar, 2014; Susanto, Chang, and Ha, 2016). Mobile banking is a personalized service, and the major barrier to its adoption is safety and privacy concerns (Afshan and Sharif, 2016). Worries about mobile banking include disclosure of personal information (53.3%), account being stolen (38.2%), and intercepted (5.8%). But some people said not to worry at all (24.7%) when they use mobile banking (TWNIC, 2016). The data show that most mobile banking users have existing concerns about privacy and security. Many bank customers have a lack of trust, lack of controllability, security issue, and concern privacy of electronic banking (Susanto, 2016; Kim, Shin, and Lee, 2009; Lee and Chung, 2009; Luarn and Lin, 2005). Therefore, there are many banking customers that still prefer ATM banking services (Shih and Fang, 2006). Mobile banking firms should emphasize the importance of security, safety, reliability and convenience (Lin, 2011). However, banking firms offer mobile banking service that not only build a safe transaction environment, but also focus on the security of personal information collection and privacy mechanism. Previous studies only discussed the trust perceived and intention of usage mobile banking (Gumussoy, 2016; Gu, Lee, and Suh, 2009) or the concern privacy and personal perceived of adopt Internet banking (Susanto, 2016; Pikkarainen, Pikkarainen, Karjaluoto, and Pahnla, 2004). Few studies have focused on the issue of privacy mechanism influence concerns for personal information, trust perceived, and risk perceived attitude.

However, the relative importance of privacy and trust regarding mobile banking may differ between potential and repeat customers. In the context of mobile banking, there is the empirical research comparing the relative important factors that influence adoption decisions

in the case of customers. As a result, a deeper understanding of privacy and trust concerns in mobile banking is needed. Motivated by these issues, this study examines the effect of the privacy mechanism (privacy policy and privacy empowerment) on attitude and behavioral intention about adopting mobile banking. From a managerial perspective, the findings should provide further insight into the significance of multifaceted strategies for understanding and managing the potential privacy issue and current mobile banking customers.

## **2. Literature**

### *2.1 Mobile Banking*

The rapid spread of Internet-enabled mobile phones and PDAs transformed banking applications on mobile devices. This is a logical evolution of electronic banking (Luo et al., 2010). Chen (2013) presented the newly emerging channels of online banking and rapidly increasing penetration rates of mobile phones. The branchless banking technology starts from the Internet and is now a widely innovative with updated mobile banking (Afshan and Sharif, 2016). Mobile banking is simply the use of cell phone stations such as mobile and PDAs to contact a banking system. Mobile banking customers can use banking facilities such as information inquiry, account managing, bill payment and money transfers etc. (Luarn and Lin, 2005).

Previous studies explore trust and use intention in mobile banking (Gumussoy, 2016; Gu et al., 2009). Susanto et al. (2016) describe initial smart phone use in banking service. It has a significant influence on security and perceived trust and satisfaction. Chen (2013) suggests that critical factors must be developed. These influence attitude and use intention in mobile banking. Gumussoy (2016) explores the factors affecting the adoption of mobile banking including continuance use intention, satisfaction, trust, process, task, technology fitness and service quality. Therefore, mobile banking is increases mobility more than traditional banking. It also increases security and privacy risks (Afshan and Sharif, 2016; Shaikh and Karjaluoto, 2015). Thus, to attract customers, mobile banking firms must emphasize the importance of securing customer confidence, safety and reliability (Lin, 2011).

### *2.2 Concern for information privacy*

Information privacy is defined by Westin (1967) as individuals interacting in groups. Information privacy can become a relevant constraint or enabler. Information privacy concerns are referred to an individual's subjective views of fairness within the context of information privacy (Campbell, 1997). It is one of the important issues for ethical, law, social, and political topics (Culnan and Bies, 2003). It explores users' information privacy concerns and has intention to expose their personal information for Internet firms. The definition of privacy concerns individuals have with the information privacy practices of organizations (Smith, Milberg, and Burke, 1996). Internet privacy concerns are a research domain. It is an issue for personal data and is really a matter of customers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared by commercial websites (Hong and Thong, 2013).

Social contract theory is especially useful for research perceptions of fairness and justice (Donaldson and Dunfee, 1994). The notion of social contract has been applied widely to explain various phenomena including the consumer-firm relationship (Dunfee, Smith, and Ross Jr, 1999). Social contract theory suggests that a firm's collection of personally identifiable data is fair only when the consumer is granted control over the information and the consumer is informed relate the firm's intended use of the information (Malhotra, Kim, and Agarwal, 2004). Malhotra et al. (2004) indicate that Internet users' information privacy concerns (IUIPC) are namely, collection, control and awareness, which exhibit desirable psychometric properties in the context of online privacy. Awareness of privacy refers to the degree to which a consumer is concerned about his/her awareness of organizational information privacy practice. Therefore, it is very important for awareness of privacy practices. Companies seeking information online should disclose the way that the data are collected, processed, and used. Online privacy policy should have a clear and conspicuous disclosure. They should be aware and knowledgeable about how personal information will be used.

Increasingly, digital and networked society has new challenges with personal information privacy (Angst and Agarwal 2009; Malhotra et al. 2004). Commercial websites seeking personal information online should disclose the way the data are collected, processed, and used (Hong and Thong, 2013). Firms use technologies such as customer relationship management to launch individually targeted marketing programs, and their information practice may conflict with the information privacy rights of customers (Son and Kim, 2008). Many Internet users are expected to adopt certain forms of behavior to protect information privacy.

Abdullah et al. (2015) shows that ease of use, customer support, privacy and transaction and payment significantly influenced customer satisfaction toward internet banking transactions. In addition, Afshan and Sharif (2016) find that mobile banking is largely a personalized service the main barriers to adoption are safety and privacy concerns. People may choose not to adopt mobile banking because of security or privacy concerns because mobile banking is relatively new and novel electronic delivery channels are offered by banks (Lin, 2011).

### *2.3 Trust and Perceived Risk Attitude*

Trust is an interaction behavior between customer and business. Trust is a long-term relationship, and transaction is a critical factor (Chaudhuri and Holbrook, 2001). Trust is also a critical point for e-commerce there are a lack of proven guarantees that the e-vendor will not engage in harmful opportunistic behaviors (Gefen, Straub, and Boudreau, 2000; Kollock, 1999; Reichheld and Schefter, 2000). Such behaviors include unfair pricing, conveying inaccurate information, violating privacy, unauthorized use of credit card information, and unauthorized tracking of transactions (Gefen, Karahanna, and Straub, 2003). A trust relationship benefits the e-vendor (Reichheld and Schefter, 2000). Prior literature shows TAM as a theoretical frame work a critical factor that reflects the user's security and privacy concerns in the customer acceptance of Internet banking (Wang, Wang, Lin, and Tang, 2003). Therefore, one reason to not use mobile banking is a lack of trust (Lin, 2011; Kim et al.,

2009; Lee and Chung, 2009). Competence, benevolence, integrity and predictability of trusting beliefs can generate trust (McKnight, Cummings, and Chervany, 1998). In the existing risk of online transactions, trust is the important construct (Reichheld and Schefer, 2000). McKnight et al. (1998) present structural assurance as one of trust. Structural assurance means that one believes that protective structure (e.g. guarantees, contracts, regulations, promises, legal recourse, processes, or procedures). Yousafzai, Pallister, and Foxall (2003) propose a conceptual model of trust with antecedents that influence customer's trust, perceived security and perceived privacy in use online banking. In the study, trust is defined as belief in the integrity, benevolence, and ability of the mobile banking service (Gefen et al., 2003). Privacy policy is one of the dimension of structural assurance. Afshan and Sharif (2016) present in the absence of customer's direct experience. They rely on structural assurance to make certain that their financial transactions on mobile are safe to process and are backed with legitimate rules and structures. This not only effectively reduces the concern for information privacy and perceived risk attitude, but also significant enhances the user's trust of mobile banking.

Perceived risk is seeking consumer behavior as risk taking (Bauer, 1960). Bauer (1960) defines perceived risk as the consumer's feeling that uncertainty relates to the consequences of transactions. Past research present the perceived risk as the customer accompanying all purchases to varying degrees and influencing buying behavior (Cox, 1964). Perceived risk may also be defined as an individual's level of control over uncertain conditions (Baird & Thomas, 1985). Perceived risk has multiple dimensions as well including social, financial, physical, psychological, time, and performance risks (Stone & Gronhaug, 1993). Therefore, it also has been identified as an influential factor in the earlier phases of the purchase process (Dowling & Staelin, 1994). Perceived risk has been widely discussed, and studies have shown that perceived risk is a critical factor influencing customer decisions and behaviors (Chen, Chen, Hsiao, and Chiu, 2016; Chen & Chang, 2012). Consumers might worry about purchasing products and services from faceless retailers, giving out personal and financial information online, buying products they cannot examine physically before a purchase, loss of time or money, as well as what the friends and family will think of their purchase (Brosdahl & Almousa, 2013).

The multi-dimension construct combine as twelve kinds of perceived risk a within commercial product (Jacoby and Kaplan, 1972). Financial risk is the potential loss of money via the purchase (Laroche, McDougall, Bergeron, and Yang, 2004). Financial risk is one of perceived risk that the product or service will not reach the expected function. Banking customers are most concerned about the financial risk, and the main reason for personal financial, transactions and payment service. Prior research has shown that the intangible nature of services makes it difficult and sometimes impossible for customers to evaluate the service offering before the purchase of the service, and after purchase and use (Mitchell & Grotorex, 1993). Anus and Qureshi, Malik, Abbasi, Chaudhry, and Mirza (2011) investigate the financial, performance, privacy, time and psychological risks facets that significantly influence the adoption of mobile banking. Financial risk is defined as the potential net loss of money, and this includes a customer's sense of insecurity regarding online credit cards,



which are seen as an obstacle to online purchasing (Maignan & Lukas, 1997). Thus, the study defines perceived risk attitude as financial risk. It explores the mobile banking customer's usage intention for using a financial function or service. When the perceived risk attitude is low, then the use intention of the customer increases. If the user has a higher concern for information privacy when he uses mobile banking, then his perceived trust reduces and perceived risk attitude increases. Therefore, in our study we hypothesized the following:

**H1.**Concerns for information privacy are negatively influenced by perceived trust of mobile banking.

**H2.**Concerns for information privacy are positively influenced by perceived risk attitude of mobile banking.

**H3.**Perceived risk attitude is negatively influenced by usage intention perceived of mobile banking.

**H4.**Perceived risk attitude has a mediator effect on concerns for information privacy and usage intention perceived of mobile banking.

#### *2.4 Privacy Mechanism*

As more and more people use mobile services, a variety of anonymous security-related solutions have been proposed to solve the privacy concerns of mobile user. Structural assurances refer to assessment of success due to safety nets such as legal recourse, guarantees, and regulations, which exist in a specific context by Gefen et al.(2003). Structural assurances can be built into the Web site such as the TURSTe seal of eTrust ([www.etrust.com](http://www.etrust.com)). The transaction process establishes the safety measures, and they are insured for customer's expectations. Strong institution perceived trust between buyer and the Internet store helps develop a guaranty procedure for the independent or semi-independent third-party assurances (Kimery & McCord, 2002). Third-party assurances use third-party technology and establish the guarantee mechanism. This has been restrained and inspected. They set the identifying icon or assurance seal. The assurance seal design is a reliability indicator to assure third-party standards and related financial services. Except third-party seal, Internet privacy right policy is one of the structural assurances. According to Hetcher (2001), offering the privacy policy is a phenomena from the 1990s many websites set the linkage in the home page. Thus, future privacy policy must be proposed as the appropriate policy for the user. Both raise the trust and effectively use the customer information in the privacy policy regulations.

Van Dyke, Midha, and Nemati (2007) define empowerment as employee empowerment and consumer empowerment. These represent the individual power transform between the highest to lowest level. The two empowerments redefine the conception for consumer privacy empowerment. Privacy empowerment is a concept for psychological. E-commerce customers control or disseminate their personal information. Firms take the initiative to explain the collection and usage for customer. They can reduce their perceived concerns (Malhotra et al., 2004). Measuring the constructs of concerns for information privacy is defined from Smith et al. (1996) as how mobile banking uses and protects the user's information privacy. Thus, the

moderator variable of privacy mechanism influences customers' perceived trust and perceived risk. Therefore in our study we hypothesize the following:

**H5.** Different privacy mechanism has a moderate effect on concerns for information privacy and perceived trust of mobile banking.

**H6.** Different privacy mechanism has a moderate effect on concerns for information privacy and perceived risk attitude of mobile banking.

### 3. Materials and Methods

As many as 425 subjects participated in the survey by answering a questionnaire. The sample is collected in Taiwan in January 2016 to February 2016 using an online questionnaire (77.6% response rate). This research uses AMOS and SPSS statistics tools analysis data. We use structural Equation Modeling (SEM). Three main aspects in the analysis are descriptive statistics, reliability and validity analysis, and SEM analysis. The study explores the different privacy mechanisms that influence perceived risk attitude and perceived trust of mobile banking customer, and usage intention perceived. The research items are coded on a five-point Likert scale ranging from strongly disagree (1) to strongly agree (5).

The measured moderate variable is adapted from Malhotra et al. (2004). It contains different situations to design the two questionnaires. It references recent privacy policy and transaction environments from physical banking. Privacy mechanisms are classified as privacy policy and empowerment. Privacy policies is adapted by Gefen et al. (2003) as the Questionnaire I. Privacy empowerment is adapted by Van Dyke et al. (2007) as the Questionnaire II (see Table 1).

Table 1. Questionnaire classification

Classification	Situation mode
Questionnaire I (Situation 1: Privacy Policy)	Mobile banking provides information privacy guarantees such as TRUSTe badges, toll-free call, legal norms or detailed privacy policies. It can ensure that the customer's personal information will not be subject to unauthorized access, abuse or trafficking. It also ensures that the information provided by customers is complete and correct.
Questionnaire II (Situation 2: Privacy Empowerment)	Mobile banking provides a privacy mechanism that allows users to choose which personal information to offer. Users have the right to determine how these personal information are used. When a customer uses a mobile banking, they can decide whether or not their information is collected and used.

The questionnaire has four parts: backgrounds; concerns for information privacy; situation assumed, perceive trust and risk for using mobile banking; and usage intention. Only the third part is different because we want to understand the diversity influenced between the privacy policy and privacy empowerment.



## 4. Data Analysis and Results

### 4.1 Description collection

The data analysis use SPSS and AMOS software with a sample size of N=425. The demographic statistics (Table 2) shows more man (56%) than women (43.76%). The age of the respondents is mostly 18-30 (74.35%) and 31-40 (21.41%) years-old. Most of the respondents (41.65%) have a monthly income of 20,001 to 40,000, and under 20,000 (36.94%). Almost all respondents have over one banking account (99.76%), and most respondents have over four bank accounts (44.24%). Most have used mobile banking (72.47%). More than 81.18% of respondents' are unwilling offer their real position information to mobile banking. The concerns for information privacy exist in all users they worry that their personal data is gathered by the other firms.

Table 2. Profile of the respondents

Measure	Items	Frequency	Percentage
Gender	Male	238	56.00%
	Female	186	43.76%
	Others	1	0.24%
Age (years)	<18	2	0.47%
	18-30	316	74.35%
	31-40	91	21.41%
	41-50	8	1.88%
	>51	8	1.88%
Monthly income	Under 20,000	157	36.94%
	20,001-40,000	177	41.65%
	40,001-60,000	64	15.06%
	60,001-80,000	15	3.53%
	80,001-100,000	8	1.88%
	Over 100,000	4	0.94%
How many account do you have the physical banking account (include Post account)?	None	1	0.24%
	One	61	14.35%
	Two	88	20.71%
	Three	87	20.47%
	Over four	188	44.24%
Do you have the experience of using mobile banking service or transaction?	Yes	308	72.47%
	No	117	27.53%
Do you agree to offer your real position information to mobile banking?	Yes	36	8.47%
	No	345	81.18%
	I don't know	44	10.35%

### 4.2 Measurement

According to Anderson and Gerbing (1988), the study adopts two phases a measurement model and a structural model to conduct the SEM analysis. The sample data is studied for discriminant validity, reliability and convergent validity. In order to deal with the issue of discriminant validity, the values in component transformation matrix are checked.

Discriminant validity makes sure that an instrument does not correlate significantly with variables from which it should differ. The resulting solution is shown in Table 3.

The value of Cronbach's  $\alpha$  for all our variables are well above the recommended level of 0.6 suggested by Nunnally (1978). Cronbach's  $\alpha$  is 0.627 to 0.917. Furthermore, the recommended criteria for composite reliability (CR) and average variance explained (AVE) state that a scale is considered reliable if it has CR above 0.7 (Bagozzi & Yi, 1988) and AVE nearly 0.5 (Fornell & Larcker, 1981). The results established that all constructs have successfully surpassed the recommended threshold and demonstrate well in terms of convergent validity. Thus the constructs can be used to analyze the conceptual model. Table 3 shows the discriminant and convergent validity.

Table 3. Results of discriminant and convergent validity

	CR	AVE	$\alpha$	CIP	PT	PRA	UIP
CIP	.916	.645	.888	(.803)	-	-	-
PT	.944	.773	.925	-.595***	(.879)	-	-
PRA	.914	.681	.882	.454***	-.409***	(.825)	-
UIP	.864	.517	.805	-.590***	.648***	-.418***	(.719)

Diagonal elements represent the average variance extracted (AVE), while off-diagonal elements represent the square correlations. Concern for information privacy (CIP), Perceived trust (PT), Perceived risk attitude (PRA), use intention perceived (UIP)

#### 4.3 Analysis of the structural model

The research model fits are  $\chi^2/df=4.347$ , Goodness-of-Fit (GFI) =0.768, Adjusted Goodness-of-Fit (AGFI) =0.789, Comparative Fit Index (CFI) =0.841, Root Mean Square Error of Approximation (RMSEA) =0.089. Overall, the goodness of fit indices are mediocre. Figure 1 shows the empirical findings of our research hypotheses.

The results show the negative significant impact of concern for information privacy (CIP) ( $\beta=-0.653$ ;  $p<0.01$ ) in perceived trust (PT), thus confirming hypotheses H1. The model explains 42.7% of the variation in perceived trust (PT). Concern for information privacy (CIP) is positively significant and influences perceived risk attitude (PRA) ( $\beta=0.557$ ,  $p<0.01$ ). This confirms hypotheses H2. The model explains 31.1% of the variation in perceived trust (PT). Perceived risk attitude (PRA) ( $\beta=-0.528$ ,  $p<0.01$ ) is statistically significant in influencing usage intention perceived (UIP). This confirms the hypotheses H3.

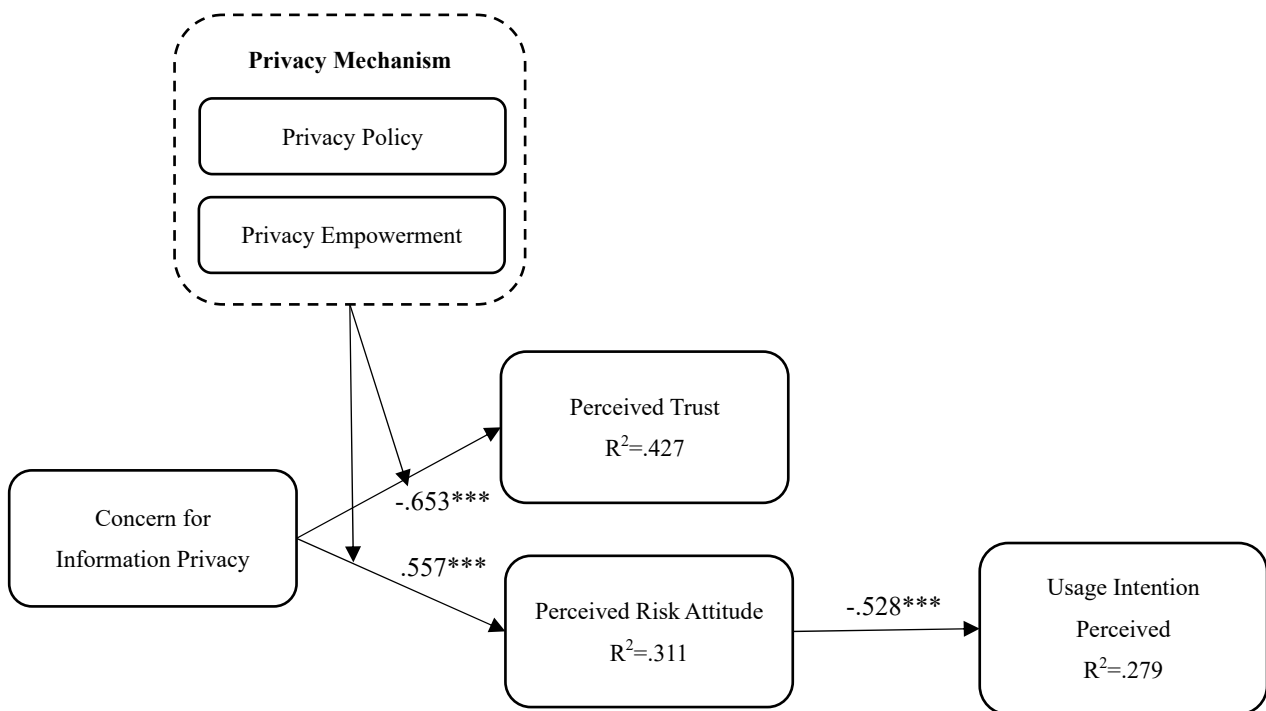


Figure 1. The structural model results [Note:\*\*\* $p < 0.01$ ]

#### 4.4 Mediator effect analysis

According to the valid method by Baron and Kenny (1986), we state the following. (1) Concern for information privacy (CIP) has significant effects of usage intention perceived (UIP) ( $\beta = -0.763$ ,  $p < 0.001$ ). (2) Concern for information privacy (CIP) has significant effects of perceived risk attitude (PRA) ( $\beta = 0.825$ ,  $p < 0.001$ ). When CIP and PRA are predicting variables, UIP is outcome variable, and mediator variable is the significant effects ( $\beta = -0.134$ ,  $p < 0.001$ ). Therefore, the influence effect of CIP is reduction ( $\beta = |-0.763|$  to  $|-0.652|$ , and the  $p$ -value is significant). This is complete mediation, and H4 is supported.

Table 4. The mediator effect analysis results

Dependent Variables	Source	Unstandardized Coefficients		Standard Coefficients	t-value	p	Model Explanations
		$\beta$	Std. Error	$\beta$			
UsageIntention Perceived	Intercept	7.298	0.239	-	30.583	0.000	F=226.360***
	Concern for Information Privacy	-0.763	0.051	-0.590	-15.045	0.000	Adjust R <sup>2</sup> =0.347
Perceived Risk Attitude	Intercept	-0.543	0.370	-	-1.468	0.143	F=110.087***
	Concern for Information Privacy	0.825	0.079	0.454	10.492	0.000	Adjust R <sup>2</sup> =0.205
UsageIntention Perceived	Intercept	7.225	0.234	-	30.841	0.000	F=127.588*** Adjust R <sup>2</sup> =0.374
	Concern for Information Privacy	-0.652	0.056	-0.505	-11.699	0.000	
	Perceived Risk Attitude	-0.134	0.031	-0.189	-4.373	0.000	

#### 4.5 Moderator effect analysis

The moderator effect analysis is referenced from Jaccard and Turrisi (2003). Adopted multiple hierarchical regression analysis validates the interaction. In this study, the privacy mechanism (moderator variable) is nominal the variable. Concern for information privacy, perceived trust and perceive risk attitude are continuous variables. Following the moderator effect analysis, there are the two groups (privacy policy and empowerment) of privacy mechanism. The regression analysis of concern for information privacy is perceived trust (Table 5).

The valid nominal variable moderator effect is according to Paternoster, Brame, Mazerolle, and Piquero (1998). The privacy policy equation is  $Y=2.075+0.137X$ , and privacy empowerment equation is  $Y=5.979-0.428X$ . Fisher's z transformation gathered the absolute value of z as above 1.96, and it is significant ( $Z=2.15836$ ). The moderation exists for concerns in information privacy and perceived trust. The privacy policy is positive and not significant ( $p=0.595$ ), but privacy empowerment is negative and significant ( $p=0.000$ ). Thus, privacy empowerment affects the customer's information privacy concerns, and influences their perceived trust. Thus, H5 is empirically confirmed.

Table 5. The moderation results of concern for information privacy and perceived trust

Privacy mechanism	Model	Unstandardized Coefficients		Standard coefficients	t-value	Sig.
		$\beta$	Std. Error	$\beta$		
Privacy Policy	(Constant)	2.057	1.271		1.618	.107
	Concern for Information Privacy	.137	.259	.035	.532	.595
Privacy Empowerment	(Constant)	5.979	.167		35.786	.000
	Concern for Information Privacy	-.428	.038	-.633	-11.379	.000

The regression analysis focuses concern for information privacy in perceived risk attitude; Table 6 displays the results. The privacy policy equation is  $Y=5.595-0.395X$ , and privacy empowerment equation is  $Y=0.217+0.614Y$ . Fisher's z transformation has gathered the absolute value of z as above 1.96, and this is significant ( $Z=-3.06049$ ). The moderation exists for concerns in information privacy and perceived trust. The privacy policy is negative and not significant ( $p=0.216$ ), then the privacy empowerment is positive and significant moderation ( $p=0.000$ ). Thus, privacy empowerment affects customer's information privacy concerns and influences their perceived trust. Thus, H6 is empirically confirmed.

Table 6. The moderation results of concerns for information privacy and perceived risk attitude

Privacy Mechanism	Model	Unstandardized Coefficients		Standard coefficients	t-value	Sig.
		$\beta$	Std. Error	$\beta$	e	
Privacy Policy	(Constant)	5.595	1.565		3.574	.000
	Concern for Information Privacy	-.395	.318	-.082	-1.240	.216
Privacy Empowerment	(Constant)	.217	.388		.561	.576
	Concern for Information Privacy	.614	.087	.451	7.033	.000

#### 4.6 Hypothesis analysis

Table 7 displays the results of our hypothesis testing. The absolute t-value is above 1.96 confirming H1, H2, and H3. Perceived risk attitude has complete mediation effect (see Table 4). This confirms hypothesis H4. Privacy policy and empowerment all have the moderator effects. This confirms the hypotheses H5 and H6 (see Table 5 and Table 6).

 Table 7. Hypothesis testing [Note:\*\*\* $p < 0.01$ ].

Hypothesis	Hypothesized path	Path coefficient	t-value	Remarks
H1	CIP → PT	-.653***	10.745	Supported
H2	CIP → PRA	.557***	9.604	Supported
H3	PRA → CIP	-.528***	-7.772	Supported
H4	Mediation of PRA	-	-	Supported
H5	Moderation of privacy policy	-	-	Supported
H6	Moderation of privacy empowerment	-	-	Supported

#### 4.7 Compare and analysis the situation models

We have two situations for privacy policy (Situation I) and privacy empowerment (Situation II). The analysis compares the different moderator effects in Table 8. The two models are both goodness-of-fit indices and optimization models.

Table 8. Compare the model of privacy mechanism

Model	$\chi^2$	df	$\chi^2/df$	GFI	AGFI	CFI	RMSEA
Situation I: Privacy policy	265.834	206	1.290	0.907	0.885	0.953	0.036
Situation II: Privacy empowerment	577.442	206	2.80	0.844	0.808	0.769	0.096

Table 9 displays the different privacy mechanisms, and it has valid hypotheses results for H1 to H6. The results are not significant in Situation I, and the hypotheses are unsupported. Therefore, the results show significant effects for Situation II, and the hypotheses are all supported.

Table 9. The results of compare the privacy mechanism

Effect Influence	Situation I: Privacy policy (N = 229)			Situation II: Privacy empowerment (N=196)		
	Path Coefficients (p)	t-value	Hypothesis Valid	Path Coefficients (p)	t-value	Hypothesis Valid
H1 CIP → PT	0.136 (.175)	1.355	unsupported	-0.739 ***	-.3885	supported
H2 CIP → PRA	-0.071 (.469)	-.724	unsupported	0.628 ***	6.216	supported
H3 PRA → CIP	-0.027 (.736)	-.337	unsupported	-0.691 ***	-3.536	supported
H4 Mediation of PRA	(.958)	-	unsupported	***	-	supported
H5 Moderation of privacy policy	(.595)	-	unsupported	***	-	supported
H6 Moderation of privacy empowerment	(.216)	-	unsupported	***	-	supported

When the privacy mechanism is the privacy policy, then the hypothesis is not significant. When the customer uses mobile banking, privacy policy has no effect on the user's privacy concerns. But it does have a significant effect on privacy empowerment. The results show that privacy empowers the customer's concerns for information privacy. This is a positive influence of usage intention in perceived and perceived risk attitude. The perceived risk attitude negatively influences usage intention.

## 5. Discussion and Conclusion

This research proposes an integrative model to provide the factors influencing the adoption of mobile banking. The findings suggested that our proposed model not only integrates the data is also empirically significant. The results explored different privacy mechanisms that influence intention of usage mobile banking. Therefore, the model has shown the significant increase in user trust perceived or reduce perceived attitude to influence usage intention perceived.

Almost all subjects (99.76%) have at least one or above personal bank account or post account many, even over four accounts (44.24%). It is the important issue with everyone. Therefore, 72.47% people have experience with mobile banking, and it is not strange to use a financial product or banking service. Therefore, most people have no awareness in sharing their personal position (81.18%). They not only worry and care about personal privacy information but also care about what information has been gathered. Mobile banking offers transfer, inquiry credit card bill, and inquiry foreign currency rate. Banking firms have to supply these three services on mobile devices.

The empirical finding also support the significant association of concerns for information privacy (CIP), perceived trust (PT), perceived risk attitude (PRA), and use intention perceived (UIP) with intention to adopt mobile banking. Highlighting the moderator and moderator is valid in this study. The present study formulated six hypotheses, and all are statistically confirmed by our data. H1 is supported that user's information privacy concerns. It is negatively influenced by the perceived risk. The use of channels of Internet or mobile communication shows that users cannot be face-to-face with a bank employee. Thus, users not only faced the uncertainty of the Internet but also have unhappy experiences, which might diminish trust. Thus, concerns in information privacy result in a positive influence on user's perceived risk attitude for using mobile banking.

We found user's information privacy concerns have a positive impact the perceived attitude. These results are similar study of Malhotra et al. (2004). The lower perceived risk attitude effectively raises the usage intention perceived for using mobile banking. It is similar to a study by Wu and Wang (2005). Mobile banking should provide convenience to their customers to eliminate the uninspiring effects of mobile phones in performing banking tasks. This invents usable and easy to use interfaces.

Following the result consequence of H4, there is the mediator effect on concerns for information privacy (CIP) and usage intention perceived (UIP). We can reduce user's perceived risk attitude to effectively reduce their information privacy concerns and raise the usage intention perceived. Via the moderator effects, the study strives to examine the different privacy mechanism in predicting usage intention perceived of individuals to adopt mobile banking. The results of H5 and H6 are similar to studies of Gefen et al. (2003) and Lauer and Deng (2007). While mobile banking may offer the complete structural assurance (e.g., strong privacy policy statement, external third-party certification) or present complete privacy empowerment environment (e.g. mobile banking may follow the rules of fair information practices to transfer the right of the user to control or disseminate personally identifiable information to individuals), it can add to the perceived trust of customer and reduce perceived risk attitude of customer to use mobile banking.

Mobile banking provides privacy empowerment of privacy mechanism to influence the user's perceived trust and perceived risk attitude. The moderation in our study shows that privacy empowerment is significantly more influential than privacy policy. This highlights the importance of privacy empowerment regarding the presence of service and third-party acknowledgement in mobile banking activities. Furthermore, the useful way offers choice and provides correct and suitable privacy empowerment to raise usage intention perceived in individuals to adopt mobile banking. Mobile banking firms should focus on designing both safe and completely private mobile banking mechanisms (e.g., firewall, security control software, detection software, or, completely working management instruction).



Recently, Fintech combined Internet and mobile technology. Fintech is an emerging financial service company that shocked the banking industry. Government policies promote financial service. Fintech presents several business including third party payment and financial investment. It not only transformed the banking service business but also changed individual lifestyles. Therefore, implementing emerging technologies can impact customer trust and risk perceptions. Moreover, micropayment, mobile payment, or financial investment applications all have information privacy concerns. Thus, the layout of developed countries promote the emerging issue as in Fintech. The financial supervisory commission in Taiwan promotes banking investment, and Fintech includes the payment processing institutions act for open banking and online business. Financial innovation investment and development is important in Taiwan given more convenient and real-time mobile transactions and services (Buzz Orange, 2016). Therefore, future research can explore the perspective for user's convenience with real time data and privacy. Mobile banking presents customized service for an individual lifestyle. It is a crucial indicator for financial integrity of financial technologies. The integrity of the infrastructure and consideration of risk control and management should focus on information privacy concerns. Both the privacy mechanism and convenience are balanced. Usage intention gives them suitable privacy empowerment for service items.

The privacy issue of financial technologies is a critical point. The individual transaction records and personal privacy have been used for counties and, financial firms. The transformation of Fintech development is a new phenomenon. Banking firms must invest to build a new system for the demands of big data analysis and information security. There are important factors for financial information technology investment growth (Market Intelligence & Consulting Institute [MIC], 2016). The core value for financial technology development suggests a complete experience for the customer. It fetches up the shortfall from recent financial services (Market Intelligence & Consulting Institute [MIC], 2015b). Fintech adopts technology innovation application to replace the parties or all function of financial business (MIC, 2015b). Both individual information privacy and services are convenient. Banking must attach importance to the user's trust and information privacy protect. The change does not always follow the past sacrifice. Personal privacy is gathered for complete services. TWNIC (2016) proposed that 56.2% of people do not want to use mobile banking because the security concern is high. The privacy concerns may make customers not want to share their information. Thus, it raises the reliability and trust. It presents the complete privacy mechanism or authorizes the level of the customer's choice. Customers can also control how personal information is used in financial firms. This builds the trust relationship and adds stickiness.

As in most empirical research, this study has several limitations. First, this study focuses on Taiwan, which a small island economy compared with other countries with, far more banking institutions. Future research can explore the antecedents and consequences of continued use of mobile banking for different countries. Second, other than the perceived trust and perceived risk attitude included here, there are still other factors influencing the customer's perceptions and behavioral intention about mobile banking. Further research considering these factors could enhance an understanding of success determinants for mobile banking. Finally, future research can explore alternate models and theories of understanding additional antecedents and constructs shaping customer information privacy concerns and intention to use mobile banking.

## References

- Abdullah, A. R., Som, N. S. M., Ibrahim, A., & Sheriff, N. M. (2015). Internet service features and satisfaction among Internet banking users. *Journal of Management Research*, 7(2), 400-410. <http://dx.doi.org/10.5296/jmr.v7i2.6944>
- Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin*, 103(3), 411-423. <http://dx.doi.org/10.1037/0033-2909.103.3.411>
- Afshan, S. & Sharif, A. (2016). Acceptance of mobile banking framework in Pakistan. *Telematics and Informatics*, 33, 370-387. <http://dx.doi.org/10.1016/j.tele.2015.09.005>
- 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.
- Anus, S., Qureshi, F. A., Malik, S., Abbasi, A., Chaudhry, A., & Mirza, S. N. (2011). Trust and initial acceptance of mobile banking in Pakistan. *International Journal of Scientific & Engineering Research*, 2(8), 337-350.
- Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science*, 16(1), 74-94. <http://dx.doi.org/10.1007/BF02723327>
- Baird, I. S., & Thomas, H. (1985). Toward a contingency model of strategic risk taking. *Academy of Management review*, 10(2), 230-243. <http://dx.doi.org/10.5465/AMR.1985.4278108>
- Bauer, R. (1960). Consumer Behavior as Risk Taking. W: Dynamic Marketing for a Changing World. Red. RS Hancock. In *Proceedings of the 43rd Conference of the American Marketing Association*, USA: Chicago.
- Brosdahl, D. J. C., & Almousa, M. (2013). Risk perception and internet shopping: comparing United States and Saudi Arabian consumers. *Journal of Management and Marketing Research*, 13, 1-17.
- BuzzOrange (2016). Taiwan Fintech transformation key here! Deloitte & Touche: new talent policy simultaneously three parallel main shaft. Retrieved from <http://buzzorange.com/techorange/2016/04/08/taiwan-fintech-future-insight/>
- Campbell, A. J. (1997). Relationship marketing in consumer markets: A comparison of managerial and consumer attitudes about information privacy. *Journal of Direct Marketing*, 11(3), 44-57. [http://onlinelibrary.wiley.com/doi/10.1002/\(SICI\)1522-7138\(199722\)11:3%3C44::AID-DIR7%3E3.0.CO;2-X/abstract](http://onlinelibrary.wiley.com/doi/10.1002/(SICI)1522-7138(199722)11:3%3C44::AID-DIR7%3E3.0.CO;2-X/abstract)
- Chaudhuri, A., & Holbrook, M. B. (2001). The chain of effects from brand trust and brand affect to brand performance: the role of brand loyalty. *Journal of marketing*, 65(2), 81-93. <http://dx.doi.org/10.1509/jmkg.65.2.81.18255>
- Chen, B. H., Chen, M. H., Hsiao, C. C., & Chiu, W. C. (2016). Antecedents and consequences of perceived corporate social responsibility on financial holding companies – Finance students' perceptions. *Journal of Management Research*, 8(3), 106-122. <http://dx.doi.org/10.5296/jmr.v8i3.9611>

- Chen, C. S. (2013). Perceived risk, usage frequency of mobile banking services. *Managing Service Quality*, 23(5), 410-436. <http://dx.doi.org/10.1108/MSQ-10-2012-0137>
- Chen, Y. S., & Chang, C. H. (2012). Greenwash and green trust: The mediation effects of green consumer confusion and green perceived risk. *Journal of Business Ethics*, 10, 1-12.
- Cox, D. F. (1964). Perceived Risk and Consumer Decision-Making: The Case of Telephone Shopping. *Journal of marketing research*, 1(4), 32-39. <http://dx.doi.org/10.2307/3150375>
- Culnan, M. J. & Bies, R. J. (2003). Consumer Privacy: Balancing Economic and Justice Considerations. *Journal of Social Issues*, 59(2), 323-342. <http://dx.doi.org/10.1111/1540-4560.00067>
- Donaldson, T., & Dunfee, T. W. (1994). Towards a unified conception of business ethics: Integrative social contracts theory. *Academy of management review*, 19(2), 252-284. <http://dx.doi.org/10.5465/AMR.1994.9410210749>
- Dowling, G. R., & Staelin, R. (1994). A model of perceived risk and intended risk-handling activity. *Journal of consumer research*, 21, 119-134. <http://dx.doi.org/10.1086/209386>
- Dunfee, T. W., Smith, N. C., & Ross Jr, W. T. (1999). Social contracts and marketing ethics. *The Journal of Marketing*, 14-32. <http://dx.doi.org/10.2307/1251773>
- Fornell, C., & Larcker, D. F. (1981). Structural equation models with unobservable variables and measurement error: Algebra and statistics. *Journal of marketing research*, 18(3), 382-388. <http://dx.doi.org/10.2307/3150980>
- Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in Online Shopping: An Integrated Model. *MIS Quarterly*, 27(1), 51-90.
- Gefen, D., Straub, D., & Boudreau, M. C. (2000). Structural equation modeling and regression: Guidelines for research practice. *Communications of the association for information systems*, 4(1), 7.
- Gu, J. C., Lee, S. C., & Suh, Y. H. (2009). Determinants of behavioral intention to mobile banking. *Expert Systems with Applications*, 36(9), 11605-11616. <http://dx.doi.org/10.1016/j.eswa.2009.03.024>
- Gumussoy, C. A. (2016). Factors affecting users' decision to continue using mobile banking in Turkey. *International Journal of Mobile Communications*, 14(4), 411-430. <http://dx.doi.org/10.1504/IJMC.2016.077341>
- Hanafizadeh, P., Keating, B. W., & Khedmatgozar, H. R. (2014). A systematic review of internet banking adoption. *Telematics and Informatics*, 31(3), 492-510. <http://dx.doi.org/10.1016/j.tele.2013.04.003>
- Hetcher, S. A. (2001). Norm Proselytizers Create a Privacy Entitlement in Cyberspace. *Berkeley Technology Law Journal*, 16(4), 877-935.
- Hong, W., & Thong, J. Y. (2013). Internet privacy concerns: an integrated conceptualization and four empirical studies. *MIS Quarterly*, 37(1), 275-298.
- Jaccard, J., & Turrisi, R. (2003). *Interaction effects in multiple regression* (No. 72). Sage.
- Jacoby, J., & Kaplan, L. B. (1972). The components of perceived risk. *Advances in consumer research*, 3(3), 382-383.

- Kim, G., Shin, B., & Lee, H.G. (2009). Understanding dynamics between initial trust and usage intentions of mobile banking. *Information Systems Journal*, 19(3), 283-311. <http://dx.doi.org/10.1111/j.1365-2575.2007.00269.x>
- Kimery, K. M., & McCord, M. (2002). Third-party assurances: Mapping the road to trust in e-retailing. JITTA. *Journal of Information Technology Theory and Application*, 4(2), 63.
- Kollock, P. (1999). The Production of Trust in Online Markets. *Advances in Group Processes*, 16, 99-123.
- Laroche, M., McDougall, G. H., Bergeron, J., & Yang, Z. (2004). Exploring how intangibility affects perceived risk. *Journal of Service Research*, 6(4), 373-389. <http://dx.doi.org/10.1177/1094670503262955>
- Lauer, T. W., & Deng, X. (2007). Building online trust through privacy practices. *International Journal of Information Security*, 6(5), 323-331. <http://dx.doi.org/10.1007/s10207-007-0028-8>
- Lee, K. C. & Chung, N. (2009). Understanding factors affecting trust in and satisfaction with mobile banking in Korea: a modified DeLone and McLean's model perspective. *Interacting with Computers*, 21 (5-6), 385-392.
- Lin, H, F. (2011). An empirical investigation of mobile banking adoption: The effect of innovation attributes and knowledge-based trust. *International Journal of Information Management*, 31(3), 252-260. <http://dx.doi.org/10.1016/j.ijinfomgt.2010.07.006>
- Luarn, P., and Lin, H. H. (2005). Toward an understanding of the behavioral intention to use mobile banking. *Computers in Human Behavior*, 21(6), 873-891. <http://dx.doi.org/10.1016/j.chb.2004.03.003>
- Luo, X., Li, H., Zhang, J., & Shim, J. P. (2010). Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: An empirical study of mobile banking services. *Decision Support Systems*, 49, 222-234. <http://dx.doi.org/10.1016/j.dss.2010.02.008>
- MIC (2015a). 2014-2015 Taiwanese Banking/ Insurance/ Securities industry's IT Spending. Taipei: Market Intelligence & Consulting Institute.
- MIC (2015b). 2016 Three trends in financial technology/ electronic payment, IoE application, API economy. Retrieved from [https://mic.iii.org.tw/micnew/IndustryObservations\\_PressRelease02.aspx?sno=415](https://mic.iii.org.tw/micnew/IndustryObservations_PressRelease02.aspx?sno=415)
- MIC(2016). The information investment arms race of financial industry: Transformation and Transboundary. Retrieved from [https://mic.iii.org.tw/micnew/Industryobservation\\_MIC02views.aspx?sno=164](https://mic.iii.org.tw/micnew/Industryobservation_MIC02views.aspx?sno=164)
- Maignan, I., & Lukas, B. A. (1997). The Nature and Social Uses of the Internet: A Qualitative Investigation. *Journal of Consumer Affairs*, 31(2), 346-371. <http://dx.doi.org/10.1111/j.1745-6606.1997.tb00395.x>
- 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. <http://dx.doi.org/10.1287/isre.1040.0032>

- McKnight, D. H., Cummings, L. L., & Chervany, N. L. (1998). Initial trust formation in new organizational relationships. *Academy of Management review*, 23(3), 473-490. <http://dx.doi.org/10.5465/AMR.1998.926622>
- Mitchell, V. W., & Greatorex, M. (1993). Risk perception and reduction in the purchase of consumer services. *Service Industries Journal*, 13(4), 179-200. <http://dx.doi.org/10.1080/02642069300000068>
- Nunnally, J. C. (1978). *Psychometric Theory*, New York: McGraw-Hill.
- Paternoster, R., Brame, R., Mazerolle, P., & Piquero, A. (1998). Using the correct statistical test for the equality of regression coefficients. *Criminology*, 36(4), 859-866. <http://dx.doi.org/10.1111/j.1745-9125.1998.tb01268.x>
- Pikkarainen, T., Pikkarainen, K., Karjaluoto, H., and Pahnla, S. (2004). Customer acceptance of online banking: an extension of the technology acceptance model. *Internet Research*, 14(3), 224-235. <http://dx.doi.org/10.1108/10662240410542652>
- Reichheld, F. F., & Scheffer, P. (2000). E-Loyalty Your Secret Weapon on the Web. *Harvard Business Review*, 78(4), 105-113.
- Shaikh, A. A., & Karjaluoto, H. (2015). Mobile banking adoption: a literature review. *Telematics and Informatics*, 32(1), 129-142. <http://dx.doi.org/10.1016/j.tele.2014.05.003>
- Shih, Y.-Y., & Fang, K. (2006). Effects of network quality attributes on customer adoption intentions of internet banking. *Total Quality Management & Business Excellence*, 17(1), 61-77. <http://dx.doi.org/10.1080/14783360500249661>
- Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: measuring individuals' concerns about organizational practices. *MIS Quarterly*, 20(2), 167-196. <http://dx.doi.org/10.2307/249477>
- Son, J. Y., & Kim, S. S. (2008). Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS Quarterly*, 15(2), 503-529.
- Stone, R. N., & Grønhaug, K. (1993). Perceived risk: Further considerations for the marketing discipline. *European Journal of marketing*, 27(3), 39-50. <http://dx.doi.org/10.1108/03090569310026637>
- Susanto, A., Chang, Y., & Ha, Y. (2016). Determinants of continuance intention to use the smartphone banking services. *Industrial Management & Data Systems*, 116(3), 508-525. <http://dx.doi.org/10.1108/IMDS-05-2015-0195>
- TWNIC (2016). A Survey on Broadband Internet Usage in Taiwan, Retrieved from <http://www.twnic.net.tw/download/200307/20160922c.pdf>
- Turban, E. King, D., Viehland, D., & Lee, J. (2006). *Electronic commerce 2006: A management perspective Pearson Education*, New Jersey.
- Van Dyke, T. P., Midha, V., & Nemati, H. (2007). The effect of consumer privacy empowerment on trust and privacy concerns in e - commerce. *Electronic Markets*, 17(1), 68-81. <https://doi.org/10.1080/10196780601136997>

Wang, Y. S., Wang, Y. M., Lin, H. H., & Tang, T. I. (2003). Determinants of user acceptance of Internet banking: an empirical study. *International Journal of Service Industry Management, 14*(5), 501-519. <http://dx.doi.org/10.1108/09564230310500192>

Westin, A. F. (1967). *Privacy and Freedom*. New York: Atheneum.

Wu, J. H., & Wang, S. C. (2005). What drives mobile commerce?: An empirical evaluation of the revised technology acceptance model. *Information & management, 42*(5), 719-729. <http://doi.ieeecomputersociety.org/10.1109/HICSS.2005.689>

Yousafzai, S. Y., Pallister, J. G., & Foxall, G. R. (2003). A proposed model of e-trust for electronic banking. *Technovation, 23*(11), 847-860. [http://dx.doi.org/10.1016/S0166-4972\(03\)00130-5](http://dx.doi.org/10.1016/S0166-4972(03)00130-5)

Zhou, T., Lu, Y., & Wang, B. (2010). Integrating TTF and UTAUT to explain mobile banking user adoption. *Computers in Human Behavior, 26*(4), 760-767. <http://dx.doi.org/10.1016/j.chb.2010.01.013>